Bezpieczeństwo OT[1] w krytycznej infrastrukturze miast inteligentnych

Analiza porównawcza wybranych incydentów bezpieczeństwa w inteligentnych sieciach energetycznych, systemach wodociągowo-kanalizacyjnych oraz inteligentnych systemach zarządzania ruchem

Simon Möhnle, Waseem Hayat
Wydział Ekonomii, Uniwersytet Dualny Badenii-Wirtembergii w Heidenheim

1. Wprowadzenie

Postępująca cyfryzacja przestrzeni miejskich prowadzi do coraz powszechniejszego powstawania tzw. inteligentnych miast, w których technologie cyfrowe są wykorzystywane do bardziej wydajnego, zrównoważonego i elastycznego zarządzania infrastrukturą miejską [1,2]. Kluczowe obszary zaopatrzenia, takie jak zaopatrzenie w energię, systemy wodociągowo-kanalizacyjne oraz systemy zarządzania ruchem, są przekształcane w systemy cyberfizyczne dzięki sieciowym czujnikom, zautomatyzowanym systemom sterowania i platformom opartym na danych. Transformacja ta wiąże się jednak z rosnącą zależnością infrastruktury krytycznej od komponentów informatycznych.

W szczególności rosnąca integracja technologii informatycznej (IT) i technologii operacyjnej (OT) powoduje, że niegdyś izolowane przemysłowe systemy sterowania są łączone w sieć za pośrednictwem dodatkowych interfejsów, przez co stają się potencjalnie podatne na ataki [3]. Podczas gdy bezpieczeństwo IT koncentruje się przede wszystkim na ochronie danych i systemów informatycznych, bezpieczeństwo OT skupia się na zapewnieniu bezpiecznego i nieprzerwanego przebiegu procesów fizycznych. Incydenty związane z bezpieczeństwem w systemach OT mogą zatem nie tylko powodować szkody cyfrowe, ale także mieć bezpośredni wpływ na ciągłość usług publicznych oraz bezpieczeństwo [4].

W tym kontekście zapewnienie bezpieczeństwa systemów OT w krytycznej infrastrukturze miast inteligentnych stanowi kluczowe wyzwanie, ponieważ czynniki techniczne, organizacyjne i strukturalne oddziałują na siebie w złożony sposób, co znacznie zwiększa potencjalną powierzchnię ataku.

Chociaż kwestia cyberbezpieczeństwa w infrastrukturach krytycznych oraz zabezpieczenia przemysłowych systemów sterowania były już przedmiotem intensywnych badań, dotychczasowe prace często prezentują perspektywę sektorową lub skoncentrowaną na technologii. Badania często skupiają się na poszczególnych obszarach infrastruktury lub konkretnych scenariuszach ataków, nie przeprowadzając przy tym analizy porównawczej różnych rodzajów infrastruktury miast inteligentnych.

W szczególności brakuje systematycznych, międzysektorowych analiz rzeczywistych incydentów bezpieczeństwa infrastruktury krytycznej, które pozwoliłyby zidentyfikować powtarzające się wektory ataku, słabości strukturalne oraz wspólne wzorce ryzyka o charakterze technologicznym i organizacyjnym. Ponadto brakuje metodologicznie spójnych analiz porównawczych, które umożliwiałyby wyciąganie z poszczególnych przypadków wniosków o charakterze ogólnym i możliwych do zastosowania w praktyce w zakresie zabezpieczania infrastruktury krytycznej.

Ta luka badawcza sprawia, że jak dotąd można jedynie w ograniczonym stopniu ustalić, jakie problemy bezpieczeństwa faktycznie powtarzają się w różnych rodzajach infrastruktury inteligentnych miast oraz jakie działania można z tego systematycznie wyprowadzić.

Celem niniejszego artykułu jest systematyczna analiza wyzwań technologicznych i organizacyjnych związanych z bezpieczeństwem OT w wybranych obszarach krytycznej infrastruktury inteligentnych miast. W tym celu analizie poddano udokumentowane rzeczywiste incydenty bezpieczeństwa dotyczące inteligentnych sieci energetycznych, systemów wodociągowo-kanalizacyjnych oraz inteligentnych systemów zarządzania ruchem.

[1] Operational Technology Security (cyberbezpieczeństwo technologii operacyjnych)

Głównym celem jest usystematyzowana identyfikacja powtarzających się wektorów ataku, typowych słabych punktów oraz ogólnych wzorców ryzyka. Na tej podstawie wyodrębnione zostają uniwersalne obszary działań technicznych i organizacyjnych, które mogą przyczynić się do poprawy zabezpieczeń systemów OT w infrastrukturze krytycznej.

W artykule zastosowano podejście oparte na porównawczych studiach przypadków w celu wskazania podobieństw i różnic między analizowanymi obszarami infrastruktury. Przedmiotem pracy nie jest opracowanie konkretnych technicznych rozwiązań wdrożeniowych ani ilościowa ocena poszczególnych środków bezpieczeństwa. Nie przeprowadzono również kompleksowej analizy wszystkich obszarów funkcjonowania inteligentnych miast, lecz świadomie skupiono się na wybranych obszarach infrastruktury mających bezpośredni związek z procesami fizycznymi.

Pytanie badawcze: W jakim stopniu analiza porównawcza wybranych incydentów bezpieczeństwa OT w inteligentnych sieciach energetycznych (Smart Grids), systemach wodociągowo-kanalizacyjnych oraz inteligentnych systemach zarządzania ruchem pozwala zidentyfikować powtarzające się wektory ataków i słabości strukturalne oraz jakie możliwe do uogólnienia obszary działania można na tej podstawie wyprowadzić w celu zabezpieczenia infrastruktury krytycznej?

2. Ramy teoretyczne i główne wyzwania

Pojęcie „smart city" odnosi się do strategicznego wykorzystania technologii cyfrowych w celu optymalizacji procesów i usług miejskich [2]. W literaturze naukowej nie ma jednak jednolitej definicji tego pojęcia. Jest to raczej szeroko rozumiana koncepcja, obejmująca wymiar technologiczny, organizacyjny i społeczny [5]. Niniejszy artykuł nie obejmuje całego spektrum cyfrowego rozwoju miast, lecz koncentruje się wyłącznie na tych elementach infrastruktury, których funkcjonowanie ma bezpośrednie znaczenie dla świadczenia usług publicznych.

Termin „infrastruktura krytyczna" odnosi się ogólnie do obiektów i systemów, których awaria mogłaby spowodować poważne zakłócenia w zaopatrzeniu, zagrożenie dla bezpieczeństwa publicznego lub inne daleko idące konsekwencje [6]. W niniejszym artykule za krytyczne uznaje się te elementy infrastruktury, które pełnią kluczową funkcję zaopatrzeniową i są oparte na cyfrowych systemach sterowania oraz komunikacji. W kontekście inteligentnego miasta oznacza to infrastrukturę jednocześnie istotną dla funkcjonowania usług publicznych i zależną od rozwiązań cyfrowych.

W tym kontekście przyjęto celowe ograniczenie analizy do trzech obszarów infrastruktury:

- Zaopatrzenie w energię w kontekście inteligentnych sieci energetycznych (Smart Grids),
- Systemy wodociągowe i kanalizacyjne,
- Inteligentne systemy zarządzania ruchem.

Systemy te charakteryzują się bezpośrednim powiązaniem z procesami fizycznymi. Komponenty cyfrowe służą tu nie tylko do przetwarzania informacji, lecz także sterują rzeczywistymi przepływami energii, dystrybucją wody czy ruchem drogowym. Incydent bezpieczeństwa może zatem nie tylko narazić dane na ujawnienie lub utratę integralności, lecz także spowodować konkretne skutki fizyczne. W niniejszym artykule nie uwzględniono czysto administracyjnych systemów informatycznych ani cyfrowych usług dla obywateli, ponieważ są one krytyczne informacyjnie, lecz nie procesowo.

Rozróżnienie między bezpieczeństwem IT a bezpieczeństwem OT

Jedną z podstaw teoretycznych stanowi rozróżnienie między technologią informacyjną (IT) a technologią operacyjną (OT). Systemy IT służą przede wszystkim do przechowywania, przetwarzania i przekazywania informacji. Typowe cele bezpieczeństwa opierają się na tzw. modelu CIA: poufność, integralność i dostępność [7].

Natomiast systemy OT sterują procesami fizycznymi lub je monitorują. Należą do nich przemysłowe systemy sterowania (ICS), systemy SCADA, sterowniki programowalne (PLC) oraz rozproszone systemy sterowania [3]. W środowiskach OT na pierwszym planie znajduje się ciągła dostępność systemów, ponieważ przerwy w działaniu mogą mieć bezpośredni wpływ na procesy fizyczne. Istotną rolę odgrywa również bezpieczeństwo funkcjonalne, ponieważ nieprawidłowe działanie może stanowić zagrożenie dla ludzi lub środowiska [4].

Dalsze różnice strukturalne utrudniają przeniesienie klasycznych środków bezpieczeństwa IT na systemy OT:

- Długie cykle życia instalacji przemysłowych (często 15–30 lat),
- zastrzeżone protokoły komunikacyjne,
- ograniczone okna na instalację poprawek i konserwację,
- wysokie wymagania dotyczące działania w czasie rzeczywistym.

Podczas gdy systemy IT można regularnie aktualizować i rekonfigurować, w środowiskach OT jest to często możliwe jedynie w ograniczonym zakresie. Środki bezpieczeństwa należy zatem wdrażać w sposób zorientowany na ryzyko i niezakłócający działalności operacyjnej. Międzynarodowe normy, takie jak IEC-62443, kładą w tym kontekście nacisk na zasady architektoniczne, takie jak segmentacja, podział na strefy oraz koncepcje „obrony w głębi” [8].

Wraz z rosnącą integracją technologii IT i OT niegdyś izolowane sieci przemysłowe są łączone dodatkowymi interfejsami z korporacyjną infrastrukturą IT, usługami w chmurze lub systemami zdalnej konserwacji. Prowadzi to do powstania nowych zależności i scenariuszy zagrożeń, które wymagają zarówno dostosowań technicznych, jak i organizacyjnych [9]. Wyraźne rozróżnienie pojęciowe i funkcjonalne między bezpieczeństwem IT a bezpieczeństwem OT jest zatem niezbędnym warunkiem dalszej analizy specyficznych wyzwań występujących w infrastrukturze inteligentnych miast.

Podstawowym problemem związanym z zabezpieczeniem technologicznym systemów OT w infrastrukturze inteligentnych miast jest długi okres eksploatacji tych systemów. Wiele przemysłowych elementów sterujących zostało pierwotnie zaprojektowanych bez uwzględnienia współczesnych cyberzagrożeń i niektóre z nich są w użyciu już od dziesięcioleci [3]. Funkcje bezpieczeństwa, takie jak silne mechanizmy uwierzytelniania czy szyfrowanie, są zatem często dostępne tylko w ograniczonym zakresie lub trudno je zintegrować w późniejszym etapie.

Z tym ściśle wiąże się ograniczona możliwość wprowadzania poprawek w środowiskach OT. W odróżnieniu od klasycznych systemów informatycznych aktualizacje lub zmiany konfiguracji nie mogą być wprowadzane bezpośrednio, ponieważ mogą one mieć bezpośredni wpływ na procesy fizyczne. Błędna aktualizacja może prowadzić do przestojów produkcyjnych lub przerw w dostawach. Operatorzy często przedkładają zatem dostępność systemu nad krótkoterminowe aktualizacje zabezpieczeń [4]. Ten konflikt celów między bezpieczeństwem a ciągłością działania utrudnia konsekwentne zarządzanie lukami w zabezpieczeniach.

Kolejne wyzwanie technologiczne wynika z postępującej konwergencji IT i OT. Inteligentne sieci energetyczne, infrastruktura wodociągowa i systemy zarządzania ruchem są obecnie często połączone z korporacyjnymi systemami IT, systemami zdalnej konserwacji lub platformami chmurowymi. Powoduje to powstanie dodatkowych punktów styku, które mogą potencjalnie służyć jako wektory ataku [9]. Badania przeprowadzone przez Europejską Agencję ds. Cyberbezpieczeństwa wskazują, że niedostatecznie zabezpieczony dostęp zdalny oraz brak segmentacji sieci należą do najczęstszych słabości w infrastrukturze miejskiej [10].

Do tego dochodzi brak przejrzystości w środowiskach systemowych, które ukształtowały się z biegiem czasu. Różni producenci, niestandardowe protokoły komunikacyjne oraz heterogeniczne komponenty utrudniają uzyskanie pełnego przeglądu istniejących zasobów i powiązań komunikacyjnych. Bez niezawodnej identyfikacji zasobów niemożliwa jest jednak ani systematyczna analiza ryzyka, ani skuteczna segmentacja [7]. Stanowi to duże wyzwanie techniczne, zwłaszcza w przypadku infrastruktury komunalnej o architekturze ukształtowanej historycznie.

Podsumowując, wyzwania technologiczne można sprowadzić do trzech kluczowych czynników: przestarzałych lub jedynie w ograniczonym zakresie modernizowalnych systemów, konfliktu celów między dostępnością a bezpieczeństwem oraz rosnącej powierzchni ataku wynikającej z coraz większej sieciowości. Na tej podstawie pojawiają się dalsze kwestie organizacyjne i strukturalne dotyczące bezpieczeństwa OT w infrastrukturze inteligentnych miast.

Oprócz czynników technologicznych to przede wszystkim warunki organizacyjne stanowią główne wyzwanie dla bezpieczeństwa OT w infrastrukturze inteligentnych miast. W odróżnieniu od klasycznych

przedsiębiorstw przemysłowych infrastruktury miejskie często charakteryzują się złożonymi strukturami. Gminy, przedsiębiorstwa komunalne, prywatni usługodawcy oraz zewnętrzni integratorzy systemów dzielą między sobą odpowiedzialność i kompetencje. Ta fragmentacja utrudnia opracowanie spójnej strategii bezpieczeństwa i często prowadzi do niejasnego podziału obowiązków w zakresie bezpieczeństwa OT [10].

Istotnym problemem jest brak jasnego podziału odpowiedzialności za bezpieczeństwo między obszarami IT i OT. Podczas gdy działy IT zazwyczaj odpowiadają za bezpieczeństwo informacji, przemysłowe systemy sterowania często leżą w zakresie odpowiedzialności technicznych działów operacyjnych. Ponieważ priorytety w obu obszarach są różne – na przykład dostępność i stabilność procesów w obszarze OT w porównaniu z ochroną danych i sieci w obszarze IT – mogą pojawić się konflikty celów [11]. Bez skoordynowanych struktur zarządzania trudno jest wdrożyć jednolitą architekturę bezpieczeństwa.

Do tego dochodzi niedobór wykwalifikowanych pracowników w dziedzinie przemysłowego cyberbezpieczeństwa. Zabezpieczenie systemów OT wymaga interdyscyplinarnej wiedzy specjalistycznej, obejmującej zarówno znajomość procesów przemysłowych, jak i kompetencje w zakresie bezpieczeństwa IT. Badania pokazują, że zwłaszcza podmioty komunalne często dysponują jedynie ograniczonymi zasobami kadrowymi do realizacji specjalistycznych zadań związanych z bezpieczeństwem OT [6]. Prowadzi to do tego, że środki bezpieczeństwa są wdrażane w sposób reaktywny, a nie strategiczny.

Kolejny czynnik organizacyjny dotyczy zarządzania ryzykiem. W wielu obszarach infrastruktury dopiero w ostatnich latach rozpoczęto systematyczne włączanie cyberbezpieczeństwa do istniejących procesów zarządzania. Międzynarodowe wytyczne podkreślają jednak, że cyberzagrożenia muszą być regularnie oceniane i uwzględniane w koncepcjach bezpieczeństwa oraz planach awaryjnych [12]. Brak lub niewystarczająca dokumentacja procesów identyfikacji ryzyka i reagowania na incydenty może w sytuacji kryzysowej prowadzić do opóźnionej reakcji.

Wreszcie wyzwaniem jest również podnoszenie świadomości pracowników. Personel techniczny w przedsiębiorstwach użyteczności publicznej zazwyczaj koncentruje się przede wszystkim na bezpiecznej eksploatacji instalacji. Cyberbezpieczeństwo jest czasami postrzegane jako dodatkowe obciążenie, zwłaszcza gdy środki bezpieczeństwa są odbierane jako utrudniające działalność. Jednak bez ugruntowanej kultury bezpieczeństwa techniczne mechanizmy ochronne mają jedynie ograniczoną skuteczność [7].

Oprócz czynników technologicznych i organizacyjnych na bezpieczeństwo OT w infrastrukturze inteligentnych miast decydujący wpływ mają ramy regulacyjne i strukturalne. Operatorzy infrastruktury krytycznej podlegają w coraz większym stopniu przepisom prawnym, które określają minimalne wymagania w zakresie bezpieczeństwa informacji i zarządzania ryzykiem. Na poziomie europejskim w szczególności dyrektywa NIS (dyrektywa w sprawie bezpieczeństwa sieci i informacji) tworzy wiążące ramy mające na celu wzmocnienie cyberbezpieczeństwa usług krytycznych [13]. Wymogi regulacyjne są transponowane do prawa krajowego i zobowiązują operatorów do wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa.

Ponadto istnieją specjalne normy i standardy dotyczące przemysłowych systemów sterowania. Na przykład seria norm IEC 62443 określa wymagania dotyczące bezpiecznych architektur, ocen ryzyka i procesów bezpieczeństwa w przemysłowych sieciach komunikacyjnych [8]. Opiera się ona na podejściu całościowym, uwzględniającym zarówno wymagania dotyczące produktów, jak i odpowiedzialność operatorów. Wdrożenie takich standardów stanowi jednak wyzwanie strukturalne, zwłaszcza dla operatorów komunalnych, ponieważ wymaga inwestycji w sprzęt, personel i procesy dokumentacyjne.

Kolejny problem strukturalny wynika z różnic w organizacji infrastruktury komunalnej. Podczas gdy duzi dostawcy energii często dysponują dobrze rozwiniętymi działami ds. bezpieczeństwa, mniejsze przedsiębiorstwa komunalne lub przewoźnicy mają bardziej ograniczone możliwości organizacyjne i finansowe. Badania dotyczące odporności infrastruktury krytycznej pokazują, że poziom bezpieczeństwa

w dużym stopniu zależy od wielkości, zasobów i dojrzałości organizacyjnej poszczególnych operatorów [6]. Skutkuje to rozdrobnieniem systemu bezpieczeństwa w obszarach miejskich.

Procesy zamówień publicznych i długoterminowe cykle inwestycyjne również wpływają na architekturę bezpieczeństwa. Ponieważ w procedurach udzielania zamówień publicznych często priorytetem jest opłacalność, wymagania bezpieczeństwa nie zawsze są uwzględniane na wczesnym etapie projektowania systemów. Jednocześnie długoterminowe umowy z dostawcami technologii utrudniają elastyczne dostosowywanie się do nowych zagrożeń [10]. Wymogi bezpieczeństwa powinny być zatem uwzględniane już na etapie planowania i zamówień, zgodnie z zasadą Security by Design.

3. Metodyka badań

Celem zastosowanego podejścia badawczego jest systematyczna identyfikacja słabych punktów bezpieczeństwa, schematów ataków oraz wyzwań strukturalnych w systemach OT krytycznej infrastruktury inteligentnych miast. Analiza rzeczywistych zdarzeń w obszarach inteligentnych sieci energetycznych, systemów wodociągowo-kanalizacyjnych oraz systemów transportowych pozwala uchwycić specyfikę poszczególnych dziedzin, a jednocześnie wyodrębnić ogólne wzorce. Studium przypadków służy zatem teorii ukierunkowanej na analizę złożonych systemów społeczno-technicznych, których zachowanie i podatność na zagrożenia można właściwie zrozumieć jedynie w kontekście rzeczywistych zdarzeń [18].

Zdecydowano się na podejście oparte na wielu studiach przypadków, ponieważ pozwala ono na analizę kilku przypadków według jednolitego schematu metodologicznego, zapewniając w ten sposób porównywalność wyników. Porównanie różnych przypadków ułatwia identyfikację powtarzających się wzorców i zwiększa teoretyczną możliwość uogólnienia uzyskanych wniosków. Wiele przypadków uznaje się za szczególnie odpowiednie do wyciągania solidnych wniosków dotyczących złożonych systemów technicznych i organizacyjnych, ponieważ uwidaczniają one zarówno podobieństwa, jak i różnice [19]. Orientacja metodologiczna jest zatem zgodna z ustalonymi standardami badań opartych na studiach przypadków.

Wybrana strategia badawcza opiera się na jakościowym projekcie badawczym opartym na wielu przypadkach, którego celem jest tworzenie teorii na podstawie badań studiów przypadków („building theory from case study research") [19, 20]. Model ten nadaje się w szczególności do dziedzin badawczych, w których istniejące teorie są jeszcze ograniczone lub fragmentaryczne oraz w których bada się złożone, zależne od kontekstu zjawiska – jak ma to miejsce w przypadku zagrożeń bezpieczeństwa OT w infrastrukturze inteligentnych miast [18]. Zamiast testować hipotezy a priori, spostrzeżenia teoretyczne wywodzi się ze szczegółowej analizy poszczególnych przypadków i stopniowo je dopracowuje w trakcie badania [19]. Połączenie analizy wewnątrzprzypadkowej (Within-Case) i porównania międzyprzypadkowego (Cross-Case) pozwala uwidocznić zarówno specyfikę poszczególnych przypadków, jak i ogólne wzorce dotyczące wektorów ataku, słabych punktów i środków zaradczych [20]. W ten sposób niniejszy artykuł dąży do uogólnienia analitycznego, a nie statystycznego, w ramach którego na podstawie konkretnych przypadków wywodzi się możliwe do uogólnienia obszary działania dla operatorów infrastruktury krytycznej [18].

Wybór przypadków odbywa się zgodnie z zasadą doboru próby teoretycznej („theoretical, not random, sampling"), zgodnie z zaleceniami dotyczącymi projektowania studiów przypadków służących budowaniu teorii. Celem nie jest uzyskanie statystycznie reprezentatywnej próby wszystkich incydentów bezpieczeństwa OT, lecz zidentyfikowanie przypadków dostarczających szczególnie bogatych informacji przydatnych do opracowania i doprecyzowania koncepcji teoretycznych. Zgodnie z tym podejściem preferowane są przypadki, które albo powielają oczekiwane wzorce w różnych kontekstach, albo charakteryzują się celowo kontrastującymi warunkami, co pozwala zbadać granice i zasadność powstającej teorii. Trzy incydenty analizowane w niniejszym artykule – atak na ukraińską sieć energetyczną, incydent w stacji uzdatniania wody w Oldsmar oraz atak na syreny alarmowe w Dallas – zostały zatem wybrane nie losowo, lecz na podstawie kryteriów merytoryczno-teoretycznych. Taka

forma doboru próby umożliwia analityczne uogólnienie wyników na podobne infrastruktury inteligentnych miast oparte na OT, nie roszcząc sobie jednak prawa do reprezentatywności statystycznej.

Wybór badanych przypadków nie jest przypadkowy, lecz opiera się na jasno zdefiniowanych kryteriach merytorycznych i metodologicznych. Celem jest wybranie takich incydentów bezpieczeństwa, które z jednej strony mają ścisły związek merytoryczny z tematem badań, a z drugiej umożliwiają rzetelną analizę porównawczą. W rozumieniu teoretycznego doboru próby wybór przypadków służy zatem ukierunkowanej analizie zdarzeń bogatych informacyjnie i istotnych z punktu widzenia celu badania [18, 19]. Pierwszym kluczowym kryterium wyboru jest związek danego incydentu z technologią operacyjną (OT). Uwzględniane są wyłącznie przypadki, w których bezpośrednio dotknięte zostały technologie operacyjne, przemysłowe systemy sterowania lub systemy sterowania procesami. Wyklucza się czysto informatyczne incydenty bezpieczeństwa bez związku z fizycznymi procesami sterowania lub monitorowania, ponieważ nie odzwierciedlają one w wystarczającym stopniu specyficznych wyzwań związanych z bezpieczeństwem OT [3, 25].

Drugim kryterium jest bezpośredni związek z procesami fizycznymi. W analizie uwzględniono wyłącznie zdarzenia, w których ataki cyfrowe mogły wywrzeć bezpośredni wpływ na procesy fizyczne, stan instalacji lub funkcje sterujące mające znaczenie dla bezpieczeństwa. Kryterium to ma kluczowe znaczenie, ponieważ w niniejszym artykule analizowane są te elementy infrastruktury inteligentnych miast, w których cyberataki mogą wywołać nie tylko skutki cyfrowe, lecz także operacyjne i społeczne konsekwencje o charakterze fizycznym.

Po trzecie, wybrane przypadki muszą dać się przyporządkować do krytycznej infrastruktury inteligentnych miast. W ramach niniejszego artykułu dotyczy to infrastruktury zaopatrzenia w energię, systemów wodociągowo-kanalizacyjnych oraz miejskich systemów ostrzegania i sterowania pełniących funkcję ochrony publicznej. Przynależność do infrastruktury krytycznej ma znaczenie, ponieważ w tym obszarze istnieje zwiększona potrzeba ochrony, a incydenty bezpieczeństwa mogą pociągać za sobą poważne konsekwencje dla bezpieczeństwa dostaw, porządku publicznego lub zaufania społecznego [6].

Kolejnym kryterium wyboru jest odpowiednia dokumentacja zdarzeń. Analizie poddawane są wyłącznie te przypadki, dla których dostępne są wiarygodne źródła pierwotne lub wtórne, na przykład w postaci raportów technicznych, oficjalnych oświadczeń, komunikatów organów nadzorczych lub uznanych w branży analiz. Kryterium to jest niezbędne, aby móc w sposób zrozumiały odtworzyć przebieg zdarzenia, słabości, skutki oraz reakcje. Niewystarczająca dokumentacja znacznie ograniczyłaby wiarygodność i trafność analizy przypadku [22, 23].

Po piąte, zwraca się uwagę na zróżnicowanie sektorowe. Wybór przypadków ma obejmować różne obszary infrastruktury, aby umożliwić zidentyfikowanie nie tylko specyficznych dla poszczególnych sektorów cech, ale także podobieństw występujących we wszystkich przypadkach. Wybór jednego przypadku z sektora energetycznego, jednego z infrastruktury wodnej oraz jednego z miejskiego systemu ostrzegania i sterowania pozwala na uwidocznienie zarówno różnic charakterystycznych dla poszczególnych rodzajów infrastruktury, jak i wspólnych wzorców podatności na ataki OT.

Wreszcie istotnym kryterium wyboru jest znaczenie teoretyczne dla dopasowywania wzorców. Przypadki dobiera się tak, aby albo potwierdzały one przewidywalne wzorce w różnych kontekstach, albo ujawniały kontrastujące przejawy tego samego podstawowego problemu. W ten sposób możliwe staje się systematyczne zestawienie struktur podatności systemów OT opisanych w literaturze z empirycznie zaobserwowanymi wzorcami przypadków [18, 20]. Wybrane przypadki mają zatem nie tylko znaczenie praktyczne, ale są również odpowiednie z teoretycznego punktu widzenia do wyodrębnienia powtarzających się wektorów ataku, strukturalnych słabości oraz obszarów działania, które można uogólnić.

Ogólnie rzecz biorąc, połączenie tych kryteriów wyboru gwarantuje, że studia przypadków są zarówno istotne pod względem tematycznym, jak i odpowiednie pod względem metodologicznym, co pozwala na uzyskanie wiarygodnej odpowiedzi na pytanie badawcze niniejszego artykułu. Wybór przypadków opiera się zatem na logice wynikającej z teorii, a jednocześnie zrozumiałej z punktu widzenia praktyki badawczej.

Niniejszy artykuł opiera się na jakościowej analizie wtórnych źródeł danych, które opisują udokumentowane incydenty bezpieczeństwa OT w krytycznej infrastrukturze inteligentnych miast. Wykorzystanie danych wtórnych jest szczególnie powszechne w badaniach nad bezpieczeństwem, ponieważ rzeczywiste cyberincydenty często nie mogą być rejestrowane bezpośrednio, a zamiast tego konieczne jest odwołanie się do opublikowanych analiz i raportów z incydentów [19, 22].

Baza danych obejmuje raporty techniczne, oficjalne badania oraz analizy przeprowadzone przez organizacje branżowe, takie jak Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz inne instytucje zajmujące się bezpieczeństwem, które dostarczają szczegółowych informacji na temat przebiegu ataków, luk w zabezpieczeniach i ich skutków [10, 25].

W celu zapewnienia rzetelności analizy stosuje się podejście oparte na triangulacji metodologicznej, polegające na wykorzystaniu kilku niezależnych źródeł dla każdego przypadku i ich wzajemnym zestawieniu. Podejście to ma na celu ograniczenie zniekształceń wynikających z poszczególnych raportów oraz odtworzenie możliwie jak najbardziej kompletnego obrazu poszczególnych incydentów bezpieczeństwa [19, 23].

Wybór konkretnych studiów przypadków opiera się na celowym zestawieniu udokumentowanych zdarzeń z różnych obszarów infrastruktury, z których każdy reprezentuje specyficzne formy ataków i słabości. Analizowane przypadki obejmują incydenty bezpieczeństwa w sektorach zaopatrzenia w energię, infrastruktury wodnej oraz systemów sterowania transportem, umożliwiając w ten sposób międzysektorową analizę zagrożeń dla bezpieczeństwa OT [16, 18].

Połączenie tych zróżnicowanych źródeł danych umożliwia przeprowadzenie analizy porównawczej, która pozwala zidentyfikować zarówno specyfikę poszczególnych przypadków, jak i ogólne wzorce. Jednocześnie należy pamiętać, że baza danych opiera się na informacjach dostępnych publicznie i w związku z tym może być niekompletna, ponieważ nie wszystkie szczegóły dotyczące incydentów bezpieczeństwa są podawane do wiadomości publicznej [20].

Ogólnie rzecz biorąc, wybrana baza danych umożliwia systematyczną i przejrzystą analizę rzeczywistych incydentów bezpieczeństwa OT, stanowiąc tym samym podstawę do późniejszej analizy obejmującej wszystkie przypadki oraz określenia obszarów działania.

Aby zapewnić systematyczną porównywalność zróżnicowanych incydentów bezpieczeństwa, analiza opiera się na standardowych ramach analitycznych. Ramy te gwarantują spójność badania we wszystkich poszczególnych przypadkach i stanowią podstawę do późniejszej analizy porównawczej [18, 19].

Analiza dokumentów odbywa się przy użyciu systemu kategorii wywiedzionego dedukcyjnie, opartego na jakościowej analizie treści zgodnie z [15]. Schemat obejmuje siedem kategorii podstawowych, które w każdym przypadku stosuje się w jednakowy sposób:

1. Kontekst i opis systemu: identyfikacja objętej incydentem infrastruktury, struktury operatora, konkretnej architektury OT oraz wykorzystywanych kanałów komunikacyjnych [18].
2. Wektor ataku i przebieg: rekonstrukcja przebiegu czasowego, począwszy od pierwszego dostępu (Initial Access), poprzez ruch lateralny (Lateral Movement), aż po manipulację procesami fizycznymi.
3. Słabości techniczne: systematyczna identyfikacja niedociągnięć technicznych, takich jak brak segmentacji sieci, niebezpieczne protokoły, niewystarczające uwierzytelnianie lub brak zarządzania poprawkami.
4. Słabości organizacyjne: analiza niedociągnięć proceduralnych, zwłaszcza w zakresie podziału ról, monitorowania bezpieczeństwa i zarządzania sytuacjami awaryjnymi.
5. Skutki: udokumentowanie technicznych, operacyjnych i społecznych konsekwencji zdarzenia, takich jak przerwy w dostawach lub zagrożenia dla bezpieczeństwa ludności.
6. Reakcja i reagowanie na incydenty: analiza podjętych działań natychmiastowych, procesu przywracania sprawności oraz jakości cyfrowej analizy śledczej.
7. Wnioski i obszary działania: opracowanie środków zapobiegawczych na poziomie technicznym, organizacyjnym i strategicznym z myślą o przyszłej infrastrukturze inteligentnych miast.

Proces analizy przebiega zgodnie ze ścisłym, wieloetapowym protokołem, mającym na celu zapewnienie rzetelności wyników zgodnie z [21]:

8. Przygotowanie i przegląd materiałów: wszystkie dokumenty zidentyfikowane w ramach gromadzenia danych zgodnie z [22] poddano pełnemu przeglądowi i uporządkowano chronologicznie.
9. Kodowanie: fragmenty tekstu istotne dla siedmiu wskazanych kategorii systematycznie wyodrębniano. Zastosowano przede wszystkim podejście dedukcyjne, zgodne z przyjętym schematem, przy czym w razie potrzeby system uzupełniano indukcyjnie o podkategorie specyficzne dla danego przypadku, aby uwzględnić specyfikę poszczególnych dziedzin, np. protokoły radiowe w sektorze transportowym [15].
10. Opracowanie ustrukturyzowanych opisów przypadków: dla każdego z trzech przypadków sporządzono szczegółową analizę, która obejmuje wszystkie kategorie schematu. Najważniejsze tezy są przy tym każdorazowo poparte źródłami pierwotnymi lub wtórnymi.
11. Syntetyzacja analityczna: wyniki podsumowano w ramach poszczególnych kategorii, aby wyraźnie wskazać najważniejsze słabości i wzorce w każdym przypadku. Stanowi to niezbędny etap przygotowawczy do późniejszej syntezy w ramach analizy międzyprzypadkowej zgodnie z [19].

4. Analiza studiów przypadków

4.1 Przypadek 1: inteligentne sieci energetyczne – atak na ukraińską sieć energetyczną (2015)

Kontekst i opis systemu. Incydent bezpieczeństwa z 23 grudnia 2015 r. uznaje się za jeden z pierwszych publicznie i wyczerpująco udokumentowanych cyberataków, w których wskutek kompromitacji systemów OT doszło do rzeczywistej awarii zasilania. Incydent objął kilku regionalnych dostawców energii na Ukrainie, których sieci dystrybucyjne były obsługiwane za pomocą przemysłowych systemów sterowania. Zaatakowana infrastruktura należy do kategorii krytycznych systemów typu „smart grid", ponieważ do sterowania operacjami przełączania, monitorowania sieci i zarządzania eksploatacją w ramach sieci dystrybucji energii elektrycznej wykorzystywano cyfrową technikę sterowania i telemechaniki [3, 4, 9, 18]. Publicznie dostępne raporty opisują środowisko, w którym klasyczne systemy informatyczne biurowe, sieci operacyjne oraz systemy sterowania zbliżone do OT były funkcjonalnie ze sobą powiązane, co stworzyło warunki do przejścia atakujących z poziomu IT na poziom OT [3, 25]. CISA opisuje ten incydent jako „nieplanowane przerwy w dostawie prądu, które dotknęły dużą liczbę klientów" w dniu 23 grudnia 2015 r.; SANS ocenia go jako skoordynowany atak na kilku ukraińskich dostawców energii elektrycznej.

Wektor ataku i przebieg. Zgodnie z łańcuchem ataku zrekonstruowanym w literaturze i raportach technicznych, incydent rozpoczął się od początkowego przejęcia kontroli nad infrastrukturą IT przedsiębiorstwa za pomocą ataku typu spear-phishing. Następnie atakujący zapewnili sobie trwałą obecność w sieci, poruszali się w jej obrębie lateralnie i uzyskali dostęp do systemów związanych ze sterowaniem siecią. W końcowej fazie wykorzystano legalne funkcje zdalnego sterowania w celu zdalnego wyłączenia stacji transformatorowych, a tym samym celowego przerwania dostaw energii elektrycznej w kilku regionach [3, 4, 18]. Atak ten nie miał zatem charakteru oportunistycznego zakłócenia, lecz był zorganizowany jako wieloetapowa i ukierunkowana operacja, która wymagała zarówno znajomości środowiska informatycznego, jak i procesów operacyjnych związanych z dystrybucją energii elektrycznej [7, 11]. Według CISA oraz raportu SANS/E-ISAC łańcuch ataku (kill chain) rozpoczął się od spear-phishingu, a następnie obejmował przejęcie kontroli nad środowiskiem informatycznym, aż po nadużycie zdalnego dostępu na poziomie systemu SCADA i sieci dystrybucyjnej.

Słabości techniczne. Analiza przypadku wskazuje na kilka słabych punktów technicznych, które umożliwiły atak lub znacząco go ułatwiły. Po pierwsze, incydent ujawnia niewystarczającą segmentację między biurową infrastrukturą IT a środowiskami sterowania operacyjnego. Po drugie, kluczową rolę odegrał zdalny dostęp, ponieważ istniejące możliwości zdalnego połączenia ułatwiły przeniknięcie do systemów operacyjnych. Po trzecie, przypadek ten wskazuje na środowisko, w którym widoczność,

wzmocnienie zabezpieczeń oraz techniczne monitorowanie komunikacji OT nie były wdrożone w wystarczającym stopniu, przez co atakujący mogli przez dłuższy czas działać niezauważenie [3, 11, 25, 27]. Ponadto środowiska OT, ze względu na długie cykle życia, zastrzeżone protokoły i ograniczone możliwości instalowania poprawek, są strukturalnie trudniejsze do zabezpieczenia niż klasyczne systemy IT, co dodatkowo zmniejsza ich odporność techniczną na ukierunkowane ataki [4, 8]. Zarówno CISA, jak i raport SANS wskazują braki w zakresie segmentacji sieci, zdalnego dostępu i widoczności specyficznej dla OT jako kluczowe wnioski wynikające z tego incydentu.

Słabości organizacyjne. Oprócz czynników technicznych przypadek ten ujawnia również wyraźne słabości organizacyjne. Czas trwania ataku oraz jego skoordynowany przebieg sugerują, że procesy wczesnego wykrywania, eskalacji i reagowania na nieprawidłowości związane z bezpieczeństwem nie były wystarczająco skuteczne. Wyraźnie widać również, że w hybrydowych środowiskach IT/OT niejasny podział obowiązków między działami bezpieczeństwa IT, eksploatacji sieci i zarządzania technicznego może negatywnie wpływać na zdolność reagowania [7, 10, 12]. Przypadek Ukrainy pokazuje zatem w sposób przykładowy, że bezpieczeństwo OT nie jest wyłącznie kwestią techniczną, ale zależy w znacznym stopniu od struktur zarządzania, procesów reagowania na incydenty oraz skoordynowanej organizacji bezpieczeństwa [6, 14]. Publiczne analizy podkreślają, że atakujący działali w sposób skoordynowany i wywierali presję na dotknięte organizacje zarówno pod względem technicznym, jak i organizacyjnym; wskazuje to na słabości w zakresie wykrywania, przygotowania i reagowania kryzysowego.

Skutki. Skutki tego incydentu były znaczące zarówno pod względem operacyjnym, jak i społecznym. Wyłączenie dotkniętych nim systemów spowodowało przerwy w dostawach energii elektrycznej, które dotknęły dużą liczbę odbiorców końcowych. Przypadek ten wyraźnie pokazuje, że cyberataki na systemy OT mogą pociągać za sobą bezpośrednie konsekwencje fizyczne i nie ograniczają się jedynie do utraty danych lub zakłóceń w działaniu systemów informatycznych [3, 4, 6]. Ponadto incydent ten miał duże znaczenie symboliczne i strategiczne, ponieważ uwidocznił na arenie międzynarodowej podatność cyfrowych infrastruktur energetycznych na ataki i wywarł trwały wpływ na dyskusję dotyczącą bezpieczeństwa inteligentnych sieci energetycznych [9, 26]. CISA informuje o dużej liczbie poszkodowanych klientów; raport SANS/E-ISAC podaje liczbę około 225 000 dotkniętych incydentem gospodarstw domowych.

Reakcja i reagowanie na incydenty. Reakcja na ten incydent pokazuje, że odporność operacyjna w środowiskach OT nie zależy wyłącznie od środków zapobiegawczych, ale także od zdolności do kontrolowanego przejścia w tryb ręczny lub alternatywny w razie awarii. W literaturze fachowej przypadek Ukrainy jest często przytaczany jako przykład tego, że ręczne operacje przełączania i redundancje operacyjne mogą odgrywać ważną rolę w przywracaniu funkcji krytycznych [3, 11, 25]. Jednocześnie przypadek ten podkreśla znaczenie cyfrowej analizy śledczej i międzysektorowego transferu wiedzy, ponieważ dopiero dzięki technicznej analizie ścieżki ataku można było wyciągnąć wiarygodne wnioski dla innych operatorów infrastruktury krytycznej [18, 19]. CISA i SANS wyraźnie przedstawiają ten incydent jako studium przypadku służące doskonaleniu wykrywania, segmentacji, planowania awaryjnego i przywracania sprawności.

Wnioski i obszary działania. Na podstawie tego przypadku można wyodrębnić kilka kluczowych obszarów działania mających na celu zabezpieczenie inteligentnych sieci energetycznych. Po pierwsze, konieczne jest konsekwentne oddzielenie sieci IT od sieci OT poprzez segmentację i tworzenie stref, aby utrudnić ruchy lateralne w kierunku operacyjnych systemów sterowania [3, 8, 27]. Po drugie, zdalny dostęp do systemów powiązanych z OT musi być ściśle kontrolowany, zabezpieczony i stale monitorowany, ponieważ w omawianym przypadku odegrał istotną rolę w operacyjnej realizacji ataku [25, 26]. Po trzecie, incydent ten wskazuje na konieczność wdrożenia monitoringu dostosowanego do potrzeb OT, który będzie w stanie rejestrować nie tylko klasyczne wskaźniki IT, ale także nietypowe wzorce sterowania i komunikacji w sieciach przemysłowych [7, 11]. Po czwarte, niezbędne są środki organizacyjne, takie jak jasny podział obowiązków, skoordynowane procesy reagowania na incydenty oraz regularne ćwiczenia, aby w razie zdarzenia móc reagować szybko i w sposób skoordynowany [6,

12]. Ogólnie rzecz biorąc, przypadek Ukrainy pokazuje, że główne zagrożenia nie wynikały z pojedynczej luki w zabezpieczeniach, lecz z połączenia ekspozycji technicznej, niewystarczającej segmentacji, podatnych kanałów zdalnego dostępu oraz niedociągnięć organizacyjnych. Ta kombinacja sprawia, że przypadek ten stanowi szczególnie odpowiedni przykład do analizy bezpieczeństwa OT w infrastrukturze inteligentnych sieci energetycznych. Oficjalne i specjalistyczne oceny prowadzą do bardzo podobnych wniosków: konieczna jest silniejsza segmentacja sieci, lepszy monitoring, wzmocnienie zabezpieczeń dostępu zdalnego oraz niezawodne procedury awaryjne.

4.2 Przypadek 2: systemy wodociągowo-kanalizacyjne – atak na stację uzdatniania wody w Oldsmar (2021)

Kontekst i opis systemu. Incydent, który miał miejsce w lutym 2021 r. w stacji uzdatniania wody miasta Oldsmar na Florydzie, stanowi wyraźny przykład podatności komunalnej infrastruktury wodociągowej na cyberataki. Incydent dotyczył zakładu uzdatniania wody, w którym wykorzystywano cyfrowe systemy sterowania i monitorowania do kontroli procesów chemicznych, stanów eksploatacyjnych oraz interwencji personelu obsługującego. W związku z tym przypadek ten należy zaklasyfikować do obszaru krytycznych systemów wodociągowo-kanalizacyjnych o bezpośrednim fizycznym związku z procesem, ponieważ zmiany parametrów sterowania mogą mieć bezpośredni wpływ na jakość wody, a tym samym na bezpieczeństwo zaopatrzenia ludności [3, 11, 25]. Z publicznie dostępnych informacji wynika, że instalacja była wyposażona w interfejsy człowiek-maszyna (HMI), komputery operatorskie działające w środowisku Windows oraz możliwości zdalnego dostępu, co umożliwiało cyfrową interakcję z parametrami istotnymi dla procesu [3, 10].

Wektor ataku i przebieg. Atak wyszedł na jaw po tym, jak operator instalacji zauważył, że kursor myszy na ekranie komputera operatorskiego poruszał się samodzielnie, a ustawienia w systemie ulegały zmianie. W trakcie tego incydentu wartość dozowania wodorotlenku sodu, stosowanego w procesach uzdatniania wody do regulacji wartości pH, została w krótkim czasie znacznie zwiększona. Zgodnie z dostępnymi raportami do tego celu wykorzystano istniejący zdalny dostęp do systemu, co oznacza, że atak nie został przeprowadzony poprzez złożone, wieloetapowe przemieszczanie się w sieci, lecz poprzez bezpośredni dostęp do systemu związanego z procesem [7, 11, 25]. Przypadek ten stanowi zatem przykład pokazujący, że w mniejszych infrastrukturach komunalnych nawet stosunkowo proste wektory ataku mogą powodować znaczne zagrożenia, jeśli istnieje bezpośredni dostęp do interfejsów użytkownika powiązanych z HMI lub SCADA [3, 26].

Luki techniczne. Analiza incydentu wskazuje na kilka luk technicznych, które umożliwiły atak lub znacząco go ułatwiły. Przede wszystkim kluczową rolę odegrało istnienie dostępnego z zewnątrz zdalnego dostępu, ponieważ umożliwiał on bezpośrednią interakcję z komputerem operatorskim istotnym dla procesu [25, 27]. Ponadto przypadek ten wskazuje na niewystarczające zabezpieczenie zdalnego dostępu, zwłaszcza w zakresie uwierzytelniania, ograniczeń dostępu oraz monitorowania aktywnych sesji [7, 8]. W publicznej dyskusji na temat tego zdarzenia regularnie wskazuje się także na słabą segmentację między administracyjnymi i operacyjnymi obszarami systemu oraz na stosowanie przestarzałych środowisk systemów operacyjnych, co prawdopodobnie dodatkowo zmniejszyło odporność techniczną na nieautoryzowany dostęp [3, 4, 11]. Przypadek ten wyraźnie pokazuje zatem, że połączenie zewnętrznego dostępu zdalnego, niewystarczającego wzmocnienia zabezpieczeń oraz ograniczonej architektury ochronnej specyficznej dla technologii operacyjnej (OT) stanowi poważne zagrożenie dla komunalnej infrastruktury wodociągowej [10, 25].

Słabości organizacyjne. Oprócz niedociągnięć technicznych incydent ten ujawnia również wyraźne słabości organizacyjne. Fakt, że interwencja o kluczowym znaczeniu dla bezpieczeństwa mogła w ogóle zostać przeprowadzona za pośrednictwem dostępu zdalnego, wskazuje na niedociągnięcia w zarządzaniu dostępem oraz w kontroli organizacyjnej dostępów uprzywilejowanych [7, 12]. Ponadto przypadek ten wskazuje, że w mniejszych placówkach gminnych środki bezpieczeństwa są często mniej sformalizowane, ograniczone pod względem kadrowym i ukierunkowane bardziej na praktyczne aspekty operacyjne niż na kwestie strategiczne [6, 10]. Jednocześnie incydent ten pokazuje, jak bardzo wykrycie

ataku w takich środowiskach może zależeć od czujności poszczególnych operatorów. Fakt, że manipulacja dawkowaniem środków chemicznych została zauważona przez pracownika i cofnięta, wskazuje, że same techniczne systemy wykrywania i alarmowe albo nie istniały, albo nie były wystarczająco skuteczne [11, 12]. Wynika z tego, że środki organizacyjne, takie jak jasny podział obowiązków, kontrolowane procesy zdalnego dostępu, szkolenia personelu oraz zdefiniowane procedury reagowania, odgrywają kluczową rolę w zapewnieniu bezpieczeństwa infrastruktury wodociągowej [14, 16].

Skutki. W tym konkretnym przypadku udało się zapobiec rzeczywistemu uszkodzeniu systemu zaopatrzenia w wodę pitną, ponieważ zmiana stężenia wodorotlenku sodu została wykryta na czas i skorygowana. Niemniej jednak potencjalna skala szkód była znaczna, ponieważ nieprawidłowe dozowanie środków chemicznych w stacjach uzdatniania wody może mieć bezpośredni wpływ na jakość wody, a tym samym na zdrowie ludności [3, 25]. Incydent ten w szczególny sposób pokazuje, że cyberataki na infrastrukturę wodociągową nie tylko powodują zakłócenia operacyjne lub techniczne, ale mogą również bezpośrednio ingerować w wrażliwe fizyczne procesy zaopatrzenia [6, 11]. Ponadto przypadek ten wywołał duże echo w mediach i na arenie politycznej, ponieważ w sposób obrazowy ujawnił, jak podatna na cyberzagrożenia może być infrastruktura komunalna dysponująca ograniczonymi zasobami [10].

Reakcja i reagowanie na incydent. Reakcja na incydent polegała na natychmiastowym cofnięciu zmanipulowanych wartości przez personel obsługujący, a także na późniejszych kontrolach stanu bezpieczeństwa i możliwości zdalnego dostępu. Z analitycznego punktu widzenia przypadek ten pokazuje, że natychmiastowa reakcja operacyjna była skuteczna, jednak rzeczywista odporność w dużym stopniu zależała od ludzkiej obserwacji i ręcznej interwencji [7, 11]. Z punktu widzenia bezpieczeństwa infrastruktury operacyjnej (OT-Security) jest to sytuacja ambiwalentna: z jednej strony dzięki interwencji personelu udało się zapobiec fizycznym szkodom, z drugiej zaś przypadek ten ujawnia, że prewencyjne techniczne i organizacyjne mechanizmy kontrolne nie były wystarczające, aby zapobiec atakowi na wczesnym etapie lub automatycznie go powstrzymać [3, 12]. W odniesieniu do reagowania na incydenty w infrastrukturze wodnej można z tego wyprowadzić wniosek, że nadzór techniczny, uregulowane procesy zdalnego dostępu oraz jasno zdefiniowane mechanizmy eskalacji muszą być ściśle ze sobą skoordynowane [25, 27].

Wnioski i obszary działania. Na podstawie przypadku Oldsmar można wyodrębnić kilka kluczowych obszarów działania mających na celu zabezpieczenie gminnych systemów wodociągowo-kanalizacyjnych. Po pierwsze, zdalny dostęp do systemów powiązanych z procesami operacyjnymi należy konsekwentnie ograniczać, technicznie zabezpieczać oraz ściśle kontrolować na poziomie organizacyjnym, ponieważ zwłaszcza w małych i średnich jednostkach infrastruktury dostęp z zewnątrz stanowi szczególnie krytyczny wektor ataku [10, 25, 27]. Po drugie, konieczna jest silniejsza segmentacja między biurową infrastrukturą IT, systemami administracyjnymi oraz systemami obsługi i sterowania powiązanymi z technologią operacyjną (OT), aby utrudnić bezpośrednią ingerencję w procesy fizyczne [3, 8]. Po trzecie, przypadek ten wskazuje na konieczność wdrożenia monitoringu dostosowanego do potrzeb OT, który wcześnie wykrywa nietypowe dostępy oraz zmiany parametrów procesowych mające krytyczne znaczenie dla bezpieczeństwa [7, 11]. Po czwarte, szczególne znaczenie mają środki organizacyjne, zwłaszcza jasne regulacje dotyczące dostępu uprzywilejowanego, podnoszenie świadomości personelu obsługującego oraz ustanowienie niezawodnych procesów reagowania na incydenty i procedur awaryjnych [6, 12]. Ogólnie rzecz biorąc, przypadek Oldsmar ma szczególną wartość naukową, ponieważ pokazuje, że poważne zagrożenia dla procesów fizycznych niekoniecznie wymagają wysoce złożonych łańcuchów ataku, lecz mogą wynikać już ze stosunkowo łatwych do wykorzystania słabości w zakresie dostępu zdalnego i organizacji. Dzięki temu przypadek ten szczególnie dobrze nadaje się do późniejszej analizy porównawczej, ponieważ stanowi kontrprzykład wobec wysoce złożonych ataków, takich jak przypadek Ukrainy, a jednocześnie pozwala dostrzec podobne podstawowe wzorce podatności OT.

4.3 Przypadek 3: inteligentne systemy zarządzania ruchem – atak na system syren alarmowych w Dallas (2017)

Kontekst i opis systemu. Incydent związany z systemem ostrzegania zewnętrznego miasta Dallas, który miał miejsce w kwietniu 2017 r., stanowi istotny przykład podatności na ataki miejskich systemów ostrzegawczych i sterujących, które w szerszym ujęciu można zaliczyć do inteligentnych systemów sterowania i alarmowych związanych z ruchem drogowym lub mających kluczowe znaczenie dla bezpieczeństwa. System, którego dotyczyło zdarzenie, stanowił obejmującą całe miasto sieć 156 syren zewnętrznych, wykorzystywanych do ostrzegania ludności przed zagrożeniami, takimi jak tornada lub inne sytuacje kryzysowe. Chociaż systemy takie nie posiadają tej samej logiki procesowej, co klasyczne systemy SCADA stosowane w infrastrukturze energetycznej lub wodociągowej, wykazują one jednak wyraźny związek z technologią operacyjną (OT), ponieważ cyfrowe lub radiowe polecenia sterujące bezpośrednio wyzwalają fizyczne sygnały ostrzegawcze w przestrzeni miejskiej [3, 4, 7]. W przypadku Dallas udokumentowano, że system ostrzegania zewnętrznego składa się ze 156 syren i służy do ostrzegania osób przebywających na zewnątrz.

Wektor ataku i przebieg zdarzenia. Incydent miał miejsce 7 kwietnia 2017 r., kiedy to wszystkie 156 syren w mieście Dallas zostało uruchomionych bez rzeczywistego zagrożenia i kilkakrotnie wywołało alarm. Zgodnie z publicznymi oświadczeniami władz miasta oraz doniesieniami mediów, uruchomienie syren nie było spowodowane klasycznym włamaniem do systemu informatycznego, lecz transmisją lub podszywaniem się pod sygnał radiowy sterujący syrenami. Atak opierał się zatem na zewnętrznym ataku radiowym, a dokładniej na pewnego rodzaju spoofingu sygnału lub mechanizmie powtórnego odtwarzania, a nie na przejęciu kontroli nad biurowym systemem IT ani na typowym przemieszczaniu się w sieci cyfrowej [7, 11]. Właśnie ten przebieg wydarzeń sprawia, że przypadek ten jest szczególnie interesujący z analitycznego punktu widzenia, ponieważ pokazuje, że problemy z bezpieczeństwem OT w infrastrukturze inteligentnych miast nie muszą koniecznie wynikać z konwergencji IT/OT, ale mogą również wynikać z niedostatecznie zabezpieczonych architektur sterowania opartych na łączności radiowej. Władze Dallas oficjalnie oświadczyły, że syreny uruchomiło „wtargnięcie”; przedstawiciele miasta oraz późniejsze doniesienia wskazywały jednak, że uruchomienie nastąpiło za pośrednictwem sfałszowanego sygnału radiowego.

Luki techniczne. Analiza zdarzenia wskazuje na kilka luk technicznych. Kluczowe znaczenie miało przede wszystkim sterowanie systemem za pomocą sygnałów radiowych. Jeśli sygnały aktywacyjne nie są wystarczająco zabezpieczone przed podszywaniem się, odtworzeniem lub nieautoryzowanym wysłaniem, już sama znajomość lub odtworzenie odpowiedniej logiki sterującej może doprowadzić do nieuprawnionego uruchomienia fizycznych systemów ostrzegawczych [4, 7]. W przypadku Dallas w publicznej dyskusji zwrócono szczególną uwagę na braki w zakresie szyfrowania, uwierzytelniania i wzmacniania sygnałów. Doprowadziło to do sytuacji, w której system był co prawda sprawny pod względem funkcjonalnym, jednak bezpieczeństwo jego komunikacji nie było wystarczająco zabezpieczone przed atakiem z zewnątrz [8, 11]. Przypadek ten ilustruje zatem słaby punkt charakterystyczny dla OT, który różni się od wcześniej rozpatrywanych przypadków: w centrum uwagi nie znalazło się nadużycie zdalnego dostępu ani przemieszczanie się przez sieć hybrydową, lecz podatność zdecentralizowanego, sterowanego radiowo systemu ostrzegawczego na poziomie protokołu i komunikacji. Raporty dotyczące tego incydentu wskazują sam sygnał radiowy jako drogę ataku; miasto Dallas natychmiast podjęło decyzję o wprowadzeniu ulepszeń w zakresie bezpieczeństwa i zapowiedziało dodatkowe środki ochronne, w tym wzmocnienie zabezpieczeń systemu.

Słabości organizacyjne. Oprócz niedociągnięć technicznych incydent ten ujawnia również braki organizacyjne. Po pierwsze, okazuje się, że w ocenie bezpieczeństwa takiego systemu najwyraźniej nie uwzględniono w wystarczającym stopniu możliwości zewnętrznego ataku radiowego. Z drugiej strony incydent ten wskazuje na braki w przygotowaniu na przypadki błędnego albo fałszywego uruchomienia systemów ostrzegawczych o szerokim zasięgu, zwłaszcza w odniesieniu do procesów komunikacji i reagowania wobec ludności, centrów dowodzenia oraz służb ratunkowych [6, 12]. Atak doprowadził nie

tylko do nieuprawnionego uruchomienia syren, ale także do znacznego obciążenia systemu numeru alarmowego, ponieważ wielu obywateli skontaktowało się z numerem alarmowym z powodu fałszywego alarmu. Pokazuje to, że odporność organizacyjna w tego typu infrastrukturach nie polega wyłącznie na technicznym zabezpieczeniu systemu źródłowego, ale musi również obejmować przygotowanie powiązanych procesów kryzysowych i komunikacyjnych [7, 10]. Doniesienia mediów i analizy wykazały, że syreny uruchamiały się wielokrotnie, a linie numeru alarmowego 911 były silnie obciążone.

Skutki. Bezpośrednimi skutkami tego zdarzenia były rozległy fałszywy alarm wśród ludności, znaczne poruszenie w mieście oraz istotne obciążenie infrastruktury numerów alarmowych. W odróżnieniu od przypadków z Ukrainy i Oldsmar, w tym incydencie na pierwszy plan nie wysuwały się bezpośrednie szkody w procesach związanych z energią lub wodą, jednak społeczne skutki ataku były znaczące. Nieuprawnione uruchomienie miejskiego systemu ostrzegawczego podważa zaufanie do niezawodności publicznej infrastruktury bezpieczeństwa i w sytuacji kryzysowej może prowadzić do tego, że prawdziwe ostrzeżenia będą traktowane mniej poważnie [6, 7]. Przypadek z Dallas pokazuje zatem, że incydenty bezpieczeństwa OT mogą mieć poważne konsekwencje społeczne i konsekwencje dla bezpieczeństwa publicznego nawet wtedy, gdy nie zakłócają klasycznego procesu zaopatrzenia. W kilku raportach jako główne skutki zdarzenia wskazano uruchomienie 156 syren, powtarzające się cykle alarmowe oraz dużą liczbę zgłoszeń na numer alarmowy.

Reakcja i reagowanie na incydenty. W perspektywie krótkoterminowej reakcja miasta Dallas polegała na wyłączeniu lub przerwaniu działania systemu syren w celu zatrzymania fałszywego alarmu, a także na podjęciu późniejszych działań technicznych i administracyjnych mających na celu wzmocnienie zabezpieczeń systemu. Z analitycznego punktu widzenia incydent ten pokazuje, że choć reakcja na incydent okazała się ostatecznie skuteczna, to jednak w warunkach czasu rzeczywistego możliwości natychmiastowego i selektywnego zablokowania nieautoryzowanych sygnałów były najwyraźniej ograniczone [11, 12]. Wskazuje to na ważny aspekt odporności w kontekście technologii operacyjnej (OT): już na etapie projektowania systemu należy uwzględnić nie tylko zapobieganie, ale także możliwość kontrolowanego wyłączenia, szybkiego przywrócenia działania oraz sprawnej komunikacji kryzysowej [3, 27]. Wkrótce po zdarzeniu miasto Dallas podjęło działania nadzwyczajne i przeznaczyło dodatkowe środki finansowe na poprawę bezpieczeństwa systemu syren.

Wnioski i obszary działania. Na podstawie przypadku z Dallas można wyodrębnić kilka kluczowych obszarów działania dotyczących zabezpieczenia miejskiej infrastruktury ostrzegawczej i sterującej opartej na technologii radiowej. Po pierwsze, bezprzewodowe protokoły sterowania i sygnały aktywacyjne muszą być konsekwentnie zabezpieczone przed spoofingiem, odtwarzaniem i nieautoryzowaną transmisją, na przykład poprzez silne uwierzytelnianie, wzmocnione mechanizmy kryptograficzne oraz systematyczne zabezpieczanie protokołów komunikacyjnych [7, 8]. Po drugie, przypadek ten pokazuje znaczenie analizy architektury pod kątem bezpieczeństwa również w odniesieniu do systemów, które nie są klasycznie postrzegane jako systemy IT, lecz których skutki fizyczne są znaczące [3, 11]. Po trzecie, incydent ten wskazuje, że koncepcje reagowania na incydenty powinny obejmować nie tylko techniczne przywracanie sprawności, ale także strategie komunikacji z ludnością i centrami zarządzania kryzysowego, aby ograniczać skutki wtórne, takie jak panika, dezinformacja czy przeciążenie powiązanej infrastruktury [6, 12]. Po czwarte, przypadek ten pokazuje, że bezpieczeństwo OT w smart city należy rozumieć szerzej niż tylko w kategoriach klasycznej konwergencji IT/OT. Również radiowe systemy ostrzegania i sterowania, nawet bez głębokiej integracji z infrastrukturą IT przedsiębiorstwa, mogą wykazywać istotne podatności bezpieczeństwa. Dlatego przypadek Dallas jest szczególnie wartościowy dla analizy międzyprzypadkowej: rozszerza perspektywę o formę miejskiej podatności OT, która nie wynika przede wszystkim z segmentacji sieci ani ze zdalnej konserwacji, lecz z niedostatecznego zabezpieczenia radiowego sterowania wywołującego skutki fizyczne. Oficjalne dokumenty i wiarygodne doniesienia potwierdzają taką interpretację, wskazując na zewnętrzną manipulację sygnałem radiowym jako przyczynę incydentu oraz na konieczność bezpośredniego wzmocnienia zabezpieczeń systemu.

5. Analiza międzyprzypadkowa i wnioski ogólne

Trzy badane przypadki różnią się pod względem sektora, architektury technicznej i konkretnego wektora ataku, ale jednocześnie wykazują kilka powtarzających się wzorców. Podczas gdy atak na ukraińską sieć energetyczną charakteryzował się wieloetapowym przejęciem kontroli nad systemami IT i OT, incydent w Oldsmar opierał się na bezpośrednim nadużyciu istniejącego zdalnego dostępu do systemu powiązanego z procesami, a przypadek w Dallas – na nieuprawnionym uruchomieniu radiowego systemu ostrzegawczego poprzez wykorzystanie luki w ścieżce komunikacyjnej [18, 19, 39–42]. Pomimo tych różnic wszystkie trzy przypadki pokazują, że to nie pojedyncza, izolowana luka, lecz współdziałanie ekspozycji technicznej, niewystarczających kontroli bezpieczeństwa i niedociągnięć organizacyjnych w znacznym stopniu sprzyjało powodzeniu ataku [3, 7, 25, 27]. Analiza porównawcza potwierdza zatem przyjęte w literaturze poświęconej bezpieczeństwu OT założenie, że ataki na infrastrukturę krytyczną zazwyczaj opierają się na kombinacjach podatności socjotechnicznych, a nie wyłącznie na pojedynczych błędach technicznych [6, 10, 11]. Przypadek na Ukrainie dotyczył skoordynowanego ataku na kilku ukraińskich dostawców energii elektrycznej, który spowodował fizyczne przerwy w dostawach prądu; przypadek w Oldsmar opierał się na nieuprawnionym dostępie do systemu SCADA w stacji uzdatniania wody; przypadek w Dallas doprowadził do nieuprawnionej aktywacji wszystkich 156 zewnętrznych syren alarmowych miasta.

Tabela 1: Matryca porównawcza analizowanych incydentów bezpieczeństwa

Kategoria analizy	Ukrainian Power Grid (2015)	Stacja uzdatniania wody w Oldsmar (2021)	Dallas Siren Hack (2017)
Sektor infrastruktury	Inteligentna sieć energetyczna / Zaopatrzenie w energię	System wodociągowo-kanalizacyjny	Inteligentny system ostrzegawczy i kierowania ruchem
Typ systemu / odniesienie do OT	SCADA, urządzenia RTU, przekaźniki zabezpieczające, centra sterowania	SCADA/HMI, terminale operatorskie oparte na systemie Windows, sterowanie procesami chemicznymi	System syren oparty na łączności radiowej z centralnym uruchamianiem
Główny wektor ataku	Spear-phishing, naruszenie bezpieczeństwa systemów informatycznych, ruch boczny w OT	Nadużycie istniejącego dostępu zdalnego	Fałszowanie sygnałów radiowych / odtwarzanie sygnałów
Słabe punkty techniczne	Brak segmentacji, niebezpieczny dostęp zdalny, ograniczona widoczność OT	Niezabezpieczony dostęp zdalny, słaba segmentacja, przestarzałe systemy	Brak lub niewystarczające uwierzytelnianie oraz zabezpieczenie sygnału radiowego
Słabe punkty organizacyjne	Ograniczone wykrywanie, niewystarczająca koordynacja między IT a OT, gotowość kryzysowa	Słabe zarządzanie dostępem, niski stopień sformalizowania, duża zależność od personelu obsługującego	Niewystarczające uwzględnienie ataków radiowych, niedociągnięcia w procesach alarmowych i komunikacyjnych
Skutki	Przerwy w dostawie prądu, duża liczba dotkniętych nimi gospodarstw domowych, duże znaczenie strategiczne	Potencjalne zagrożenie dla jakości wody pitnej, duże zainteresowanie ze strony polityków	Fałszywe alarmy, przeciążenie numerów alarmowych, utrata zaufania do infrastruktury ostrzegawczej
Reagowanie na incydenty	Ręczne przywracanie danych, analiza kryminalistyczna, wnioski wyciągnięte na poziomie poszczególnych sektorów	Ręczna korekta przez personel obsługujący, kontrola połączeń zdalnych	Wyłączenie/przerwanie pracy systemu, utwardzanie końcowe
Główne obszary działania	Segmentacja, monitorowanie OT, wzmocnienie zabezpieczeń dostępu zdalnego, procedury awaryjne	Zabezpieczenie/minimalizacja ryzyka związanego z dostępem zdalnym, monitorowaniem i zarządzaniem	Zabezpieczanie protokołów bezprzewodowych, uwierzytelnianie, komunikacja kryzysowa

5.1 Dopasowanie wzorców

Zgodnie z koncepcją dopasowywania wzorców (Pattern-Matching) według Yina analiza obejmująca różne przypadki służy do porównania empirycznie zaobserwowanych wzorców z teoretycznie przewidywalnymi strukturami podatności systemów OT [18]. Na podstawie literatury można było oczekiwać w szczególności trzech wzorców: po pierwsze, wpływu na bezpieczeństwo wynikającego z niedostatecznie kontrolowanych interfejsów między systemami wewnętrznymi a zewnętrznymi; po drugie, ograniczonej możliwości przeniesienia klasycznych środków bezpieczeństwa IT na środowiska OT; oraz po trzecie, dużego znaczenia czynników organizacyjnych dla zapobiegania i reagowania [3, 10, 25, 27].

Pierwszy wzorzec wyraźnie potwierdza się we wszystkich trzech przypadkach, choć w różnym stopniu. W przypadku Ukrainy przejście ze środowiska biurowej infrastruktury IT do środowiska OT było możliwe dzięki niedostatecznie zabezpieczonym granicom sieciowym i dostępom operacyjnym; w przypadku Oldsmar istniejący dostęp zdalny stanowił bezpośrednią drogę do systemu powiązanego z procesami produkcyjnymi; w przypadku Dallas nie był to klasyczny dostęp sieciowy, lecz niedostatecznie zabezpieczony kanał komunikacji radiowej [39–42]. Przypadki te potwierdzają zatem ogólny wzorzec, zgodnie z którym ataki na systemy OT często rozpoczynają się tam, gdzie systemy sterowania są dostępne za pośrednictwem zewnętrznych, administracyjnych lub bezprzewodowych kanałów komunikacyjnych. CISA opisuje w przypadku Ukrainy wieloetapowe przejęcie kontroli, które doprowadziło do awarii zasilania; CISA/FBI/EPA opisują w przypadku Oldsmar nieuprawniony dostęp do systemu SCADA; w przypadku Dallas odnotowano nieuprawnione uruchomienie syren w wyniku zewnętrznej ingerencji.

Drugi wzorzec dotyczy ograniczonej skuteczności czysto klasycznych zasad bezpieczeństwa IT w kontekście OT. Chociaż znane zasady bezpieczeństwa, takie jak uwierzytelnianie, kontrola dostępu i separacja sieci, odgrywają rolę we wszystkich przypadkach, to jednak w każdym z nich pojawia się kontekst specyficzny dla danego procesu i architektury. W przypadku Ukrainy efekt operacyjny był możliwy dopiero dzięki nadużyciu rzeczywistych funkcji sterujących na poziomie OT; w Oldsmar zmanipulowano parametr krytyczny dla procesu; w Dallas słabość w ścieżce sygnałowej doprowadziła bezpośrednio do fizycznego uruchomienia systemu ostrzegawczego [7, 8, 11]. Wynika z tego, że bezpieczeństwa OT nie można postrzegać wyłącznie jako rozszerzenia bezpieczeństwa IT, lecz wymaga ono funkcjonalnego spojrzenia na procesy fizyczne, ścieżki komunikacyjne i warunki operacyjne [3, 4].

Trzeci wzorzec dotyczy czynników organizacyjnych i strukturalnych. We wszystkich trzech przypadkach skuteczność ataku wynikała nie tylko z uwarunkowań technicznych, lecz została również wzmocniona przez ograniczone zarządzanie bezpieczeństwem, niewystarczające przygotowanie na sytuacje awaryjne albo brak bądź niewystarczającą skuteczność procesów monitorowania i reagowania [6, 10, 12]. Szczególnie wyraźnie widać to w przypadku Oldsmar, gdzie bezpośrednie zapobieżenie szkodom zależało w znacznym stopniu od czujności operatora, a także w przypadku Dallas, gdzie atak miał skutki uboczne dla struktur obsługi połączeń alarmowych i komunikacji kryzysowej [41,42]. Wyniki te potwierdzają założenie, że bezpieczeństwo OT w krytycznej infrastrukturze inteligentnych miast zależy w znacznym stopniu od dojrzałości organizacyjnej operatorów i nie można go zapewnić wyłącznie za pomocą technicznych środków ochronnych. Po incydencie w Oldsmar agencje CISA/FBI/EPA podkreśliły znaczenie kontroli dostępu i środków bezpieczeństwa w sektorze wodnym; po incydencie w Dallas podjęto bezpośrednie działania modernizacyjne w zakresie bezpieczeństwa systemu syren alarmowych.

5.2 Modele wyjaśniające i mechanizmy

Wykraczając poza zwykłą identyfikację wspólnych wzorców, analiza międzyprzypadkowa ma na celu uwidocznienie leżących u ich podstaw wzorców wyjaśniających. Trzy przypadki sugerują, że powodzenie ataku opierało się w każdym z nich na wspólnym mechanizmie: cyfrowa lub radiowa ścieżka dostępu umożliwiła oddziaływanie na proces fizyczny, przy czym jednocześnie występowały braki w zabezpieczeniach technicznych i słabości organizacyjne. Mechanizm ten można zatem opisać jako połączenie dostępności, niewystarczającej kontroli i fizycznej skuteczności procesu [7, 18, 19].

W przypadku Ukrainy mechanizm ten przejawia się w połączeniu naruszenia bezpieczeństwa systemów informatycznych, braku wyraźnego oddzielenia systemów OT oraz nadużycia legalnych funkcji sterujących. Atak był niezwykle złożony, ale jego powodzenie wynikało ostatecznie z tego, że dostęp cyfrowy był możliwy nawet w środowiskach procesowych i nie był tam skutecznie ograniczany [39, 40]. W przypadku Oldsmar ten sam podstawowy mechanizm był widoczny w znacznie prostszej formie: zdalny dostęp umożliwił bezpośredni dostęp do interfejsu operatorskiego powiązanego z procesem, co stworzyło możliwość manipulacji parametrami chemicznymi [41]. Z kolei w przypadku Dallas ścieżka dostępu nie była oparta na sieci, lecz na technologii radiowej; mechanizm pozostał jednak podobny, ponieważ niedostatecznie zabezpieczony kanał komunikacyjny wywołał bezpośredni skutek fizyczny w przestrzeni miejskiej [42].

Na tej podstawie można wyprowadzić drugi model wyjaśniający: im bliżej fizycznego procesu znajduje się ścieżka komunikacyjna lub zdalnego dostępu, tym mniejsza jest tolerancja systemu na błędy i tym większy jest wpływ naruszenia bezpieczeństwa. Wzorzec ten wyjaśnia, dlaczego nawet stosunkowo proste formy ataku – na przykład niewystarczająco kontrolowany dostęp zdalny lub sygnał radiowy, który można podrobić – mogą mieć poważne konsekwencje, mimo że pod względem technicznym wydają się mniej złożone niż wieloetapowe ataki typu APT [3, 11].

Trzeci model wyjaśniający dotyczy roli odporności organizacyjnej. Przypadki te pokazują, że niedociągnięcia techniczne mają szczególnie poważne konsekwencje, gdy organizacje nie dysponują jasno określonymi obowiązkami w zakresie bezpieczeństwa, odpowiednimi mechanizmami monitorowania oraz niezawodnymi procedurami awaryjnymi [6, 12]. Z tego wynika analitycznie, że podatność krytycznej infrastruktury inteligentnych miast jest nie tylko funkcją stosowanej technologii, ale także jej osadzenia instytucjonalnego i operacyjnego. Właśnie w tym tkwi główny wkład niniejszego artykułu: poszczególne przypadki pokazują różne formy ataków, jednak analiza międzyprzypadkowa ujawnia, że leżą u ich podstaw wspólne mechanizmy socjotechniczne.

5.3 Podsumowanie wyników dotyczących wszystkich przypadków

Poniższe ustalenia stanowią główne podsumowanie analityczne niniejszego artykułu. Podczas gdy rekonstrukcja poszczególnych zdarzeń opiera się na udokumentowanych źródłach pierwotnych i wtórnych, poniższe wnioski wynikają z porównawczej oceny trzech studiów przypadków w ramach analizy międzyprzypadkowej. Nie jest to zatem zwykłe podsumowanie literatury, lecz samodzielnie opracowane wnioski dotyczące wszystkich przypadków, oparte na systematycznym porównaniu badanych incydentów bezpieczeństwa.

Po pierwsze: punkty przejściowe, interfejsy i ścieżki dostępu stanowią główny obszar podatności na ataki w krytycznej infrastrukturze miast inteligentnych. Analiza porównawcza przypadków pokazuje, że we wszystkich trzech przypadkach powodzenie ataku wynikało w znacznej mierze z wykorzystania konkretnej ścieżki dostępu. W przypadku Ukrainy było to

przejście z biurowej infrastruktury IT do środowiska OT, w przypadku Oldsmar – istniejący zdalny dostęp do systemu powiązanego z procesami, a w przypadku Dallas – niedostatecznie zabezpieczony kanał sterowania oparty na łączności radiowej. Analiza międzyprzypadkowa sugeruje zatem, że luki o największym znaczeniu dla bezpieczeństwa nie leżą przede wszystkim w poszczególnych komponentach, lecz w przejściach między poziomami systemów, ścieżkami komunikacyjnymi i interfejsami sterowania. Wyniki te pozwalają uogólnić poszczególne przypadki do nadrzędnego wzorca, zgodnie z którym łączność i dostępność stanowią główne punkty wejścia dla cyberataków wywołujących skutki fizyczne.

Po drugie: powodzenie ataku nie wynika z pojedynczych, odizolowanych słabości, lecz z połączenia niedociągnięć technicznych i organizacyjnych. Porównanie tych trzech przypadków pokazuje, że same słabości techniczne nie wyjaśniają w wystarczającym stopniu przebiegu zdarzeń. We wszystkich przypadkach wyraźnie widać było, że niewystarczające uwierzytelnianie, brak segmentacji lub niezabezpieczone kanały komunikacji współdziałały z czynnikami organizacyjnymi, takimi jak niejasny podział kompetencji, ograniczony nadzór bezpieczeństwa, słabe zarządzanie dostępem lub niewystarczające przygotowanie na sytuacje kryzysowe. Przeprowadzona przez nas analiza międzyprzypadkowa prowadzi zatem do wniosku, że incydenty bezpieczeństwa OT w krytycznej infrastrukturze inteligentnych miast należy postrzegać jako zdarzenia zakłócające o charakterze socjotechnicznym. Podatność wynika nie tylko z technicznych właściwości systemów, ale również z ich osadzenia organizacyjnego oraz dojrzałości instytucjonalnej struktur operatorskich.

Po trzecie: wektory ataku, które można wykryć na wczesnym etapie, występują przede wszystkim tam, gdzie można systematycznie identyfikować nietypowe dostępy, nietypowe zmiany w procesach lub nietypowe polecenia sterujące. Analiza międzyprzypadkowa pokazuje, że zasadniczo we wszystkich trzech przypadkach można wskazać punkty wyjścia umożliwiające wcześniejsze wykrycie. W przypadku Ukrainy potencjalnymi wskaźnikami anomalii byłyby nietypowe przepływy danych między obszarami IT i OT, w przypadku Oldsmar – nietypowe ingerencje w parametry dozowania substancji chemicznych, a w przypadku Dallas – nietypowe sygnały aktywacji systemu ostrzegawczego. Wynika z tego odrębny wniosek analityczny, że możliwość wczesnego wykrycia zależy w mniejszym stopniu od absolutnej złożoności ataku, a w większym od tego, czy operatorzy są w stanie systematycznie monitorować odchylenia istotne dla bezpieczeństwa wzdłuż ścieżek komunikacyjnych i sterujących o krytycznym znaczeniu dla procesu. Właśnie w tym miejscu rozpoczyna się wyznaczanie wiarygodnych obszarów działania dla operatorów i gmin.

Podsumowując, analiza międzyprzypadkowa pokazuje, że trzy badane zdarzenia, mimo różnic sektorowych i technicznych, wskazują na wspólne podstawowe wzorce. Wkład niniejszego artykułu polega na tym, że nie tylko opisuje on te podobieństwa w odniesieniu do poszczególnych przypadków, ale także systematycznie je uogólnia i wyodrębnia jako wnioski mające zastosowanie do wszystkich przypadków w zakresie bezpieczeństwa OT w krytycznej infrastrukturze inteligentnych miast.

6. Obszary działania, ujęcie teoretyczne i podsumowanie

Niniejszy artykuł nie ma na celu opracowania konkretnych, pojedynczych środków technicznych, lecz wyodrębnienie uniwersalnych obszarów działania oraz teoretycznie ugruntowanych wniosków dotyczących powiązań na podstawie analizy porównawczej udokumentowanych incydentów bezpieczeństwa. Wkład naukowy polega zatem na wyodrębnieniu z poszczególnych przypadków uogólnialnych wzorców typowych konstelacji podatności w krytycznej infrastrukturze miast inteligentnych [18–20].

Podstawą poniższych rozważań są wnioski o charakterze ogólnym, zidentyfikowane w ramach analizy międzyprzypadkowej: szczególna podatność punktów styku i ścieżek dostępu na zagrożenia, wzajemne oddziaływanie niedociągnięć technicznych i organizacyjnych oraz znaczenie wykrywania anomalii w kontekście procesów.

Poniższe obszary działania wynikają z porównawczej syntezy trzech przeanalizowanych przypadków. Podczas gdy literatura i źródła dotyczące poszczególnych przypadków posłużyły do rekonstrukcji i klasyfikacji, to właśnie ich systematyczne ujęcie w postaci uniwersalnych obszarów działania stanowi oryginalny wkład niniejszego artykułu [18, 19].

Analiza pokazuje, że we wszystkich trzech przypadkach atak był możliwy dzięki konkretnej ścieżce dostępu: przejściu między systemami IT i OT w przypadku Ukrainy, zdalnemu dostępowi w przypadku Oldsmar oraz radiowemu kanałowi sterującemu w przypadku Dallas. Wynika z tego, że architektury bezpieczeństwa muszą być projektowane nie tyle w oparciu o komponenty, co o interfejsy. Szczególnie podatne na ataki są zatem zdalne dostępy, interfejsy konserwacyjne, dostępy do centrów kontroli oraz bezprzewodowe kanały komunikacyjne. Z technicznego punktu widzenia oznacza to segmentację, tworzenie stref, uwierzytelnianie oraz restrykcyjne kontrole dostępu [3, 8, 25, 27].

Kolejnym kluczowym wnioskiem jest to, że powodzenie ataku nie wynikało wyłącznie ze słabych punktów technicznych. We wszystkich przypadkach słabości techniczne były wzmacniane przez niedociągnięcia organizacyjne, takie jak niejasny podział kompetencji, słabe zarządzanie dostępem czy niewystarczające przygotowanie na sytuacje kryzysowe. Bezpieczeństwo OT należy zatem postrzegać jako zadanie zarządcze o charakterze socjotechnicznym. Do głównych obszarów działania należą: jasna koordynacja obowiązków w zakresie IT i OT, sformalizowanie dostępu uprzywilejowanego oraz odporne struktury reagowania na incydenty i zarządzania kryzysowego [6, 10, 12].

Analiza porównawcza przypadków pokazuje ponadto, że we wszystkich trzech przypadkach występowały anomalie możliwe zasadniczo do wczesnego wykrycia, takie jak nietypowe przepływy między obszarami IT i OT, nietypowe zmiany parametrów procesowych lub nietypowe sygnały aktywacyjne. Wynika z tego konieczność wprowadzenia monitoringu dostosowanego do potrzeb OT, który rejestruje nie tylko zdarzenia sieciowe, ale także polecenia sterujące, zmiany wartości procesowych oraz nietypowe stany pracy [7, 11, 25].

W końcu wszystkie trzy przypadki pokazują, że skutki szkody zależą w znacznym stopniu od jakości reakcji. Kluczową rolę odegrało w każdym z tych przypadków ręczne przywrócenie sprawności, natychmiastowa interwencja personelu obsługującego lub szybkie odłączenie zainfekowanego systemu. Wynika z tego, że bezpieczeństwo OT musi być postrzegane nie tylko w kategoriach prewencyjnych, ale także z uwzględnieniem odporności. Konieczne są jasne procedury eskalacji, przygotowane alternatywne tryby pracy oraz niezawodne procesy komunikacyjne [3, 6, 12].

Ogólnie rzecz biorąc, wyodrębnione obszary działania wskazują, że bezpieczeństwo OT w krytycznej infrastrukturze miast inteligentnych można skutecznie zapewnić jedynie poprzez wielopoziomową współpracę obejmującą zabezpieczenie interfejsów, wdrożenie organizacyjne, monitorowanie i odporność.

Na podstawie wyników analizy wszystkich przypadków można sformułować kilka tez w ramach analizy studiów przypadków służącej tworzeniu teorii. Nie służą one uogólnieniu statystycznemu, lecz teoretycznemu ujęciu typowych związków przyczynowych [18–20].

Teza 1: Im łatwiejszy jest dostęp do systemów OT krytycznej infrastruktury miast inteligentnych poprzez zewnętrzne, międzysystemowe lub bezprzewodowe ścieżki dostępu, tym większa jest ich podatność na cyberataki wywołujące skutki fizyczne.

Teza 2: Skuteczność ataków na bezpieczeństwo OT w krytycznej infrastrukturze miast inteligentnych wynika w znacznym stopniu z połączenia słabych punktów technicznych i niedociągnięć organizacyjnych.

Teza 3: Im bliżej fizycznego procesu znajduje się podatna na atak ścieżka komunikacyjna lub sterująca, tym większa jest potencjalna skala szkód, nawet w przypadku stosunkowo prostych form ataku.

Teza 4: Wczesne wykrywanie ataków na systemy OT zależy w znacznym stopniu od tego, czy nietypowe dostępy, nietypowe polecenia sterujące oraz nietypowe zmiany w procesach zachodzące wzdłuż ścieżek krytycznych dla procesu są systematycznie monitorowane.

Teza 5: Odporność krytycznej infrastruktury inteligentnego miasta zależy nie tylko od środków zapobiegawczych, ale również od zdolności do kontrolowanego przejścia w tryb bezpiecznej lub alternatywnej eksploatacji w przypadku awarii.

6.1 Umiejscowienie w literaturze

Wyniki uzyskane w ramach studiów przypadków i analizy międzyprzypadkowej można zaklasyfikować zarówno do literatury poświęconej bezpieczeństwu OT/ICS, jak i do badań dotyczących inteligentnych miast oraz infrastruktury krytycznej. Celem niniejszego rozdziału jest porównanie własnych ustaleń z istniejącymi podejściami naukowymi i normatywnymi oraz wskazanie ich konkretnego wkładu.

W literaturze poświęconej bezpieczeństwu systemów OT/ICS podkreśla się, że przemysłowe systemy sterowania i kontroli podlegają szczególnym zasadom bezpieczeństwa, których nie da się w prosty sposób wyprowadzić z klasycznych podejść do bezpieczeństwa IT [3, 4, 11, 25]. W szczególności wysokie wymagania dotyczące dostępności, długie cykle życia, protokoły zastrzeżone oraz ograniczone możliwości instalowania poprawek charakteryzują sytuację w zakresie bezpieczeństwa środowisk OT [3, 7]. Wyniki niniejszego artykułu wyraźnie potwierdzają to podstawowe założenie.

Jednym z kluczowych wniosków płynących z analizy porównawczej jest to, że przejścia, punkty styku i ścieżki dostępu stanowią główny obszar podatności na zagrożenia. Ustalenie to jest zgodne z zasadami segmentacji, tworzenia stref i kontrolowanych relacji komunikacyjnych, ugruntowanymi w literaturze poświęconej bezpieczeństwu OT/ICS [8, 27]. Niniejszy artykuł rozszerza jednak tę perspektywę, wykazując, że interfejsy o krytycznym znaczeniu dla bezpieczeństwa obejmują nie tylko klasyczne przejścia między systemami IT a OT, ale także dostęp zdalny oraz kanały sterowania oparte na łączności radiowej.

Również drugie spostrzeżenie, a mianowicie współdziałanie niedociągnięć technicznych i organizacyjnych, jest zgodne z dotychczasową literaturą. Wytyczne i standardy podkreślają, że techniczne środki ochronne są skuteczne tylko wtedy, gdy uzupełniają je odpowiednie procesy organizacyjne, modele ról i procedury bezpieczeństwa [3, 12, 25]. Niniejszy artykuł potwierdza ten pogląd na podstawie rzeczywistych incydentów i pokazuje, że udane ataki opierają się zazwyczaj na połączeniu podatności technicznej i słabych punktów organizacyjnych.

Ponadto wyniki potwierdzają znaczenie zdolności wykrywania i monitorowania procesów, podkreślane w literaturze poświęconej bezpieczeństwu OT. We wszystkich trzech przypadkach udało się zidentyfikować potencjalne sygnały wskazujące na nietypowe polecenia sterujące, nietypowe zmiany w procesie lub nietypowe wzorce komunikacji [7, 11, 25]. Artykuł potwierdza zatem ustalenia dotychczasowej literatury, a jednocześnie przenosi je na kontekst różnych sektorów i odmiennych rodzajów infrastruktury inteligentnych miast.

W literaturze poświęconej koncepcji „smart city” przestrzenie miejskie opisuje się przede wszystkim jako systemy połączone cyfrowo, oparte na danych i zintegrowane w sposób

międzysektorowy [1, 2, 5]. Natomiast literatura dotycząca infrastruktury krytycznej podkreśla szczególne znaczenie społeczne tych systemów, których awaria może mieć poważne konsekwencje dla bezpieczeństwa dostaw i porządku publicznego [6]. Wyniki niniejszego artykułu łączą obie te perspektywy, pokazując, że cyfryzacja infrastruktury miejskiej tworzy nowe, podatne na zagrożenia struktury łączności, które w obszarach krytycznych mogą wywoływać bezpośrednie skutki fizyczne i społeczne.

Istotnym wkładem niniejszego artykułu jest uzupełnienie często raczej abstrakcyjnej dyskusji na temat inteligentnych miast o konkretną perspektywę opartą na przypadkach związanych z bezpieczeństwem. Podczas gdy literatura poświęcona inteligentnym miastom często skupia się na potencjale innowacyjnym i wzroście wydajności [1, 2], niniejsza analiza, opierając się na rzeczywistych incydentach bezpieczeństwa, pokazuje, że cyfryzacja miejska staje się krytyczna dla bezpieczeństwa właśnie wtedy, gdy jest powiązana z systemami OT i procesami fizycznymi.

Jednocześnie artykuł ten potwierdza kluczowe założenia literatury poświęconej infrastrukturze krytycznej (CI), zgodnie z którymi podatność na zagrożenia nie wynika wyłącznie ze słabych punktów technicznych, lecz z wzajemnego oddziaływania czynników technicznych, organizacyjnych i instytucjonalnych [6]. Analiza międzyprzypadkowa pokazuje ponadto, że w kontekście inteligentnych miast podejście międzysektorowe jest szczególnie pouczające, ponieważ mimo różnic specyficznych dla poszczególnych rodzajów infrastruktury pozwala zidentyfikować wspólne wzorce podatności.

Podsumowując, niniejszy artykuł potwierdza kluczowe założenia zawarte w literaturze poświęconej bezpieczeństwu OT/ICS, inteligentnym miastom oraz infrastrukturze krytycznej (CI), zwłaszcza w odniesieniu do znaczenia interfejsów, podatności socjotechnicznych oraz wymagań dotyczących odporności. Jego oryginalny wkład polega jednak na analizie porównawczej rzeczywistych incydentów bezpieczeństwa OT, które miały miejsce w różnych obszarach krytycznej infrastruktury inteligentnych miast, oraz na wynikającym z niej międzysektorowym uogólnieniu wspólnych wzorców i obszarów działania.

6.2 Podsumowanie, ograniczenia i perspektywy

Celem niniejszego artykułu było zidentyfikowanie, poprzez analizę porównawczą wybranych incydentów bezpieczeństwa OT w inteligentnych sieciach energetycznych (Smart Grids), systemach wodociągowo-kanalizacyjnych oraz inteligentnych systemach zarządzania ruchem, powtarzających się wektorów ataku, słabości strukturalnych oraz wynikających z nich obszarów działania. Aby odpowiedzieć na pytanie badawcze, przeanalizowano atak na ukraińską sieć energetyczną (2015 r.), incydent w zakładzie wodociągowym w Oldsmar (2021 r.) oraz atak na system syren w mieście Dallas (2017 r.), a następnie poddano je porównawczej ocenie w ramach analizy międzyprzypadkowej.

Wyniki pokazują, że rzeczywiście można zidentyfikować powtarzające się wzorce we wszystkich trzech przypadkach. Szczególnie wyraźnie widać było, że przejścia, punkty styku i ścieżki dostępu stanowią główny obszar podatności krytycznej infrastruktury miast inteligentnych. Ponadto okazało się, że udane ataki nie wynikają wyłącznie z luk technicznych, ale są często ułatwiane przez współdziałanie niedociągnięć technicznych i organizacyjnych. Wreszcie analiza wykazała, że wektory ataku możliwe do wczesnego wykrycia zasadniczo istnieją, o ile nietypowe dostępy, niezwykłe polecenia sterujące lub nietypowe zmiany w procesach są systematycznie monitorowane.

Na podstawie tych ustaleń udało się wyodrębnić kilka obszarów działania, które można uogólnić. Należą do nich w szczególności zabezpieczenie interfejsów i ścieżek dostępu, ściślejsza integracja technicznych i organizacyjnych mechanizmów bezpieczeństwa, stworzenie zdolności

monitorowania i wykrywania dostosowanych do procesów, a także planowanie na wypadek awarii i przywrócenia działania ukierunkowane na odporność. Na pytanie badawcze można zatem odpowiedzieć, że analiza porównawcza rzeczywistych incydentów bezpieczeństwa OT pozwala na zidentyfikowanie powtarzających się wektorów ataku i strukturalnych słabości, a także na wyodrębnienie z nich uniwersalnych obszarów działania służących zabezpieczeniu krytycznej infrastruktury inteligentnych miast.

Znaczenie niniejszego artykułu jest ograniczone przez kilka czynników. Po pierwsze, analiza opiera się na niewielkiej liczbie trzech przypadków, przez co wyniki mają charakter teoretyczny, ale nie są reprezentatywne pod względem statystycznym. Po drugie, praca opiera się na wtórnych źródłach danych, których kompletność zależy od opublikowanej dokumentacji poszczególnych zdarzeń. Po trzecie, różnorodność analizowanych infrastruktur utrudnia pełną porównywalność przypadków, choć właśnie ta różnorodność okazała się cenna dla analizy międzyprzypadkowej. Wreszcie w niniejszym artykule nie dokonano empirycznej oceny skuteczności konkretnych działań; wyprowadzone obszary działania pozostają zatem na poziomie koncepcyjnym.

W ramach przyszłych badań warto rozszerzyć zakres analizowanych przypadków na inne elementy infrastruktury inteligentnych miast oraz zweryfikować przedstawione tutaj wnioski poprzez dodatkowe studia przypadków, wywiady z ekspertami lub badania ilościowe. Sensowne byłoby również silniejsze powiązanie z uznanymi modelami oceny stopnia dojrzałości lub ramami bezpieczeństwa, aby jeszcze bardziej skonkretyzować praktyczną przydatność uzyskanych wyników.

W praktyce niniejszy artykuł pokazuje, że bezpieczeństwo OT w inteligentnych miastach nie może być postrzegane jako odizolowana, specjalistyczna kwestia techniczna. Konieczne jest raczej zintegrowane podejście do bezpieczeństwa, łączące wzmocnienie zabezpieczeń technicznych, zarządzanie organizacyjne, monitorowanie procesów oraz planowanie awaryjne ukierunkowane na odporność. Postępująca cyfryzacja infrastruktury miejskiej jeszcze bardziej zwiększy znaczenie tych zagadnień. Niniejszy artykuł podkreśla zatem konieczność postrzegania rzeczywistych incydentów bezpieczeństwa nie tylko jako pojedynczych przypadków, ale jako empirycznej podstawy do systematycznego rozwoju architektur bezpieczeństwa krytycznej infrastruktury inteligentnych miast.

Bibliografia

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi. “Internet of Things for Smart Cities.” IEEE Internet of Things Journal, Vol. 1, No. 1, 2014, pp. 22–32.

[2] S. E. Bibri. Smart Sustainable Cities of the Future. Springer, 2018.

[3] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn. Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev. 2. National Institute of Standards and Technology, 2015.

[4] E. Knapp, J. Langill. Industrial Network Security. Syngress, 2014.

[5] C. Harrison et al. “Foundations for Smarter Cities.” IBM Journal of Research and Development, Vol. 54, No. 4, 2010.

[6] S. Bauer, M. Bötticher. Critical Infrastructure Protection. Springer, 2017.

[7] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

[8] International Electrotechnical Commission (IEC). IEC 62443 – Industrial communication networks – Network and system security. IEC Standard Series.

[9] M. H. Cintuglu, O. A. Mohammed, K. Akkaya. “A Survey on Smart Grid Cyber-Physical System Testbeds.” IEEE Communications Surveys & Tutorials, 2017.

[10] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Cities. ENISA Report, 2019.
[11] R. Krutz. Industrial Control Systems Security. Wiley, 2016.
[12] International Organization for Standardization (ISO). ISO/IEC 27001: Information Security Management Systems. ISO Standard.
[13] European Union. Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive). Official Journal of the European Union, 2016.
[14] N. Döring. Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften. 6., vollständig überarbeitete und erweiterte Auflage. Springer, 2023.
[15] P. Mayring. Qualitative Inhaltsanalyse: Grundlagen und Techniken. 12. Auflage, Beltz, 2015.
[16] M. Q. Patton. Qualitative Research & Evaluation Methods. 4th ed., Sage, 2015.
[17] C. Helfferich. Die Qualität qualitativer Daten. 5. Auflage, Springer VS, 2019.
[18] R. K. Yin. Case Study Research and Applications: Design and Methods. 6th ed., Sage, 2018.
[19] K. M. Eisenhardt. Building Theories from Case Study Research. Academy of Management Review, 14(4), 532–550, 1989.
[20] K. M. Eisenhardt and M. E. Graebner. Theory Building from Cases: Opportunities and Challenges. Academy of Management Journal, 50(1), 25–32, 2007.
[21] U. Kuckartz. Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung. Beltz Juventa, 2018.
[22] G. A. Bowen. Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2), 27–40, 2009.
[23] U. Flick. Qualitative Sozialforschung: Eine Einführung. Rowohlt, 2014.
[24] S. Lamnek. Qualitative Sozialforschung. 5. Auflage, Beltz, 2010.
[25] National Institute of Standards and Technology (NIST). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Revision 2, 2015.
[26] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Grids. ENISA Report, 2019.
[27] International Electrotechnical Commission (IEC). IEC 62443 Series: Industrial communication networks – IT security for networks and systems. Parts 1-1, 2-1, 3-3, 4-1.
[28] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber-Attack Against Ukrainian Critical Infrastructure. Alert (IR-ALERT-H-16-056-01), U.S. Department of Homeland Security, 2016.
[29] E-ISAC and SANS ICS. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems, 2016.
[30] U.S. Department of Homeland Security. Assessment of Electricity Disruption Incident Response Capabilities. 2017.
[31] Pinellas County Sheriff's Office. Press Conference on Oldsmar Water Treatment Facility Cyber Intrusion. Pinellas County, Florida, 2021.
[32] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Environmental Protection Agency (EPA). Compromise of U.S. Water Treatment Facility. Joint Cybersecurity Advisory, 2021.
[33] Cybersecurity and Infrastructure Security Agency (CISA). Top Cyber Actions for Securing Water Systems. CISA Guidance, 2021.
[34] City of Dallas. Emergency Supplemental Addendum. Dallas City Council Meeting Documents, April 12, 2017.

[35] City of Dallas Office of Emergency Management. Outdoor Warning System. City of Dallas, 2017.
[36] Associated Press. “Lack of encryption blamed for false Dallas emergency sirens.” Associated Press, April 11, 2017.
[37] A. Greenberg. “That Dallas Siren Hack Wasn’t Novel—It Was Just Really Loud.” Wired, April 10, 2017.
[38] A. Greenberg. “This Radio Hacker Could Hijack Citywide Emergency Sirens to Play Any Sound.” Wired, August 1, 2018.
[39] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber-Attack Against Ukrainian Critical Infrastructure. IR-ALERT-H-16-056-01, U.S. Department of Homeland Security, 2016.
[40] M. Assante, R. M. Lee, T. Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E-ISAC) and SANS ICS, 2016.
[41] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Environmental Protection Agency (EPA). Compromise of U.S. Water Treatment Facility. Joint Cybersecurity Advisory AA21-042A, 2021.
[42] City of Dallas. Emergency Supplemental Addendum. Dallas City Council Meeting Documents, April 12, 2017.

OT-Security in kritischen Smart-City-Infrastrukturen

Eine vergleichende Analyse ausgewählter Sicherheitsvorfälle in Smart Grids, Wasser- und Abwassersystemen sowie intelligenten Verkehrsleitsystemen

Simon Möhnle , Waseem Hayat
Fakultät Wirtschaft, Duale Hochschule Baden-Württemberg Heidenheim

1. Einleitung

Die fortschreitende Digitalisierung urbaner Räume führt zur zunehmenden Etablierung sogenannter Smart Cities, in denen digitale Technologien eingesetzt werden, um städtische Infrastrukturen effizienter, nachhaltiger und adaptiver zu steuern [1, 2]. Zentrale Versorgungsbereiche wie die Energieversorgung, Wasser- und Abwassersysteme sowie Verkehrsleitsysteme werden dabei durch vernetzte Sensorik, automatisierte Steuerungen und datenbasierte Plattformen zu cyber-physischen Systemen weiterentwickelt. Diese Transformation geht jedoch mit einer steigenden Abhängigkeit kritischer Infrastrukturen von informationstechnischen Komponenten einher.

Insbesondere die zunehmende Integration von Informationstechnologie (IT) und Operationstechnologie (OT) führt dazu, dass ehemals isolierte industrielle Steuerungssysteme über zusätzliche Schnittstellen vernetzt und damit potenziell angreifbar werden [3]. Während sich IT-Security primär auf den Schutz von Daten und Informationssystemen konzentriert, liegt der Fokus der OT-Security auf der Gewährleistung sicherer und kontinuierlicher physischer Prozesse. Sicherheitsvorfälle in OT-Systemen können daher nicht nur digitale Schäden verursachen, sondern unmittelbare physische Auswirkungen auf die öffentliche Versorgung und Sicherheit haben [4].

Vor diesem Hintergrund stellt die Absicherung von OT-Systemen in kritischen Smart-City-Infrastrukturen eine zentrale Herausforderung dar, da technische, organisatorische und strukturelle Faktoren in komplexer Weise miteinander interagieren und potenzielle Angriffsflächen erheblich erweitern.

Obwohl Cybersecurity in kritischen Infrastrukturen sowie die Absicherung industrieller Kontrollsysteme bereits intensiv untersucht wurden, zeigen bestehende Arbeiten häufig eine sektorale oder technologiezentrierte Perspektive. Studien fokussieren sich oftmals auf einzelne Infrastrukturbereiche oder spezifische Angriffsszenarien, ohne eine vergleichende Betrachtung unterschiedlicher Smart-City-Infrastrukturen vorzunehmen.

Insbesondere fehlt es an systematischen, sektorübergreifenden Analysen realer OT-Sicherheitsvorfälle, die wiederkehrende Angriffsvektoren, strukturelle Schwachstellen sowie gemeinsame technologische und organisatorische Risikomuster identifizieren. Darüber hinaus besteht ein Defizit hinsichtlich methodisch nachvollziehbarer Cross-Case-Analysen, die es ermöglichen, aus Einzelfällen generalisierbare und übertragbare Erkenntnisse für die Absicherung kritischer Infrastrukturen abzuleiten.

Diese Forschungslücke führt dazu, dass bislang nur eingeschränkt nachvollziehbar ist, welche Sicherheitsprobleme in unterschiedlichen Smart-City-Infrastrukturen tatsächlich wiederkehrend auftreten und welche Maßnahmen sich daraus systematisch ableiten lassen.

Ziel der vorliegenden Arbeit ist es, die technologischen und organisatorischen Herausforderungen der OT-Security in ausgewählten kritischen Smart-City-Infrastrukturen systematisch zu analysieren. Hierzu werden dokumentierte reale Sicherheitsvorfälle in den Bereichen Smart Grids, Wasser- und Abwassersysteme sowie intelligente Verkehrsleitsysteme untersucht.

Im Mittelpunkt steht dabei die strukturierte Identifikation wiederkehrender Angriffsvektoren, typischer Schwachstellen sowie übergreifender Risikomuster. Auf dieser Grundlage sollen übertragbare sicherheitstechnische und organisatorische Handlungsfelder abgeleitet werden, die zur Verbesserung der Absicherung von OT-Systemen in kritischen Infrastrukturen beitragen können.

Die Arbeit verfolgt einen vergleichenden Fallstudienansatz, um Gemeinsamkeiten und Unterschiede zwischen den betrachteten Infrastrukturbereichen herauszuarbeiten. Nicht Gegenstand der Arbeit ist die Entwicklung konkreter technischer Implementierungslösungen oder die quantitative Bewertung einzelner Sicherheitsmaßnahmen. Ebenso erfolgt keine vollständige Betrachtung aller Smart-City-Domänen, sondern eine bewusste Fokussierung auf ausgewählte Infrastrukturbereiche mit direktem physischem Prozessbezug.

Forschungsfrage: Inwiefern lassen sich durch eine vergleichende Analyse ausgewählter OT-Sicherheitsvorfälle in den OT-Systemen Smart Grids, Wasser- und Abwassersysteme sowie intelligente Verkehrsleitsysteme wiederkehrende Angriffsvektoren und strukturelle Schwachstellen identifizieren, und welche generalisierbaren Handlungsfelder können daraus für die Absicherung kritischer Infrastrukturen abgeleitet werden?

2. Theoretischer Rahmen und zentrale Herausforderungen

Der Begriff der Smart City beschreibt die strategische Nutzung digitaler Technologien zur Optimierung urbaner Prozesse und Dienstleistungen [2]. In der wissenschaftlichen Literatur existiert jedoch keine einheitliche Definition. Vielmehr handelt es sich um ein breit gefasstes Konzept, das technologische, organisatorische und gesellschaftliche Dimensionen umfasst [5]. In der vorliegenden Arbeit steht nicht das gesamte Spektrum der digitalen Stadtentwicklung im Fokus, sondern ausschließlich Infrastrukturen, deren Funktionsfähigkeit unmittelbar für die öffentliche Daseinsvorsorge relevant ist.

Der Begriff „kritische Infrastruktur" bezeichnet allgemein Einrichtungen und Systeme, deren Ausfall zu erheblichen Versorgungsengpässen, Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde [6]. In dieser Arbeit werden solche Infrastrukturen als kritisch verstanden, die sowohl eine zentrale Versorgungsfunktion erfüllen als auch durch digitale Steuerungs- und Kommunikationssysteme geprägt sind. Übertragen auf den Smart-City-Kontext

bedeutet dies, dass es sich um Infrastrukturen handeln muss, die eine zentrale Versorgungsfunktion erfüllen und durch digitale Steuerungs- und Kommunikationssysteme geprägt sind.

Vor diesem Hintergrund erfolgt eine bewusste Eingrenzung auf drei Infrastrukturbereiche:

- Energieversorgung im Sinne intelligenter Stromnetze (Smart Grids),
- Wasser- und Abwassersysteme,
- Intelligente Verkehrsleitsysteme.

Diese Systeme zeichnen sich durch einen direkten physischen Prozessbezug aus. Digitale Komponenten dienen hierbei nicht nur der Informationsverarbeitung, sondern steuern auch reale Energieflüsse, die Wasserverteilung oder Verkehrsströme. Ein Sicherheitsvorfall kann somit nicht nur Daten kompromittieren, sondern auch konkrete physische Auswirkungen verursachen. Rein administrative IT-Systeme oder digitale Bürgerdienste werden in dieser Arbeit nicht betrachtet, da sie informationskritisch, jedoch nicht prozesskritisch sind.

Abgrenzung zwischen IT-Security und OT-Security

Eine der theoretischen Grundlagen bildet die Unterscheidung zwischen Information Technology (IT) und Operational Technology (OT). IT-Systeme dienen in erster Linie der Speicherung, Verarbeitung und Übertragung von Informationen. Typische Schutzziele orientieren sich am sogenannten CIA-Modell: Vertraulichkeit, Integrität und Verfügbarkeit [7].

OT-Systeme steuern oder überwachen dagegen physische Prozesse. Zu ihnen zählen industrielle Kontrollsysteme (ICS), SCADA-Systeme, speicherprogrammierbare Steuerungen (PLCs) und verteilte Kontrollsysteme [3]. In OT-Umgebungen steht die kontinuierliche Verfügbarkeit der Systeme im Vordergrund, da Unterbrechungen unmittelbare Auswirkungen auf physische Prozesse haben können. Funktionale Sicherheit spielt ebenfalls eine wesentliche Rolle, da Fehlfunktionen Menschen oder die Umwelt gefährden können. [4].

Weitere strukturelle Unterschiede erschweren die Übertragbarkeit klassischer IT-Sicherheitsmaßnahmen auf OT-Systeme:

- Lange Lebenszyklen industrieller Anlagen (oft 15–30 Jahre),
- proprietäre Kommunikationsprotokolle,
- eingeschränkte Patch- und Wartungsfenster,
- hohe Anforderungen an Echtzeitfähigkeit.

Während IT-Systeme regelmäßig aktualisiert und neu konfiguriert werden können, ist dies in OT-Umgebungen häufig nur eingeschränkt möglich. Sicherheitsmaßnahmen müssen daher risikoorientiert und betriebsschonend implementiert werden. Internationale Standards wie die IEC-62443 betonen in diesem Zusammenhang architektonische Prinzipien wie Segmentierung, Zonenbildung und Defense-in-Depth-Konzepte [8].

Durch die zunehmende IT- und OT-Nutzung werden ehemals isolierte industrielle Netzwerke über zusätzliche Schnittstellen mit der Unternehmens-IT, Cloud-Diensten oder Fernwartungssystemen verbunden. Dadurch entstehen neue Abhängigkeiten und Bedrohungsszenarien, für die sowohl

technische als auch organisatorische Anpassungen erforderlich sind. [9]. Eine klare begriffliche und funktionale Trennung von IT- und OT-Security ist daher eine wesentliche Voraussetzung, um die spezifischen Herausforderungen in Smart-City-Infrastrukturen weiter analysieren zu können.

Ein grundlegendes Problem der technologischen Absicherung von OT-Systemen in Smart-City-Infrastrukturen ist die lange Lebensdauer solcher Systeme. Viele industrielle Kontrollkomponenten wurden ursprünglich ohne Berücksichtigung moderner Cyberbedrohungen entwickelt und sind teilweise seit Jahrzehnten im Einsatz [3]. Sicherheitsfunktionen wie starke Authentifizierungsmechanismen oder Verschlüsselung sind daher häufig nur eingeschränkt vorhanden oder nachträglich schwer integrierbar.

Damit eng verbunden ist die eingeschränkte Patchbarkeit von OT-Umgebungen. Anders als bei klassischen IT-Systemen können Updates oder Konfigurationsänderungen nicht ohne Weiteres durchgeführt werden, da sie unmittelbare Auswirkungen auf physische Prozesse haben können. Ein fehlerhaftes Update kann zu Produktionsausfällen oder Versorgungsunterbrechungen führen. Betreiber priorisieren daher oftmals die Systemverfügbarkeit gegenüber kurzfristigen Sicherheitsaktualisierungen [4]. Dieser Zielkonflikt zwischen Sicherheit und Betriebskontinuität erschwert ein konsequentes Schwachstellenmanagement.

Eine weitere technologische Herausforderung ergibt sich aus der zunehmenden Konvergenz von IT und OT. Smart Grids, Wasserinfrastrukturen und Verkehrsleitsysteme sind heute oft mit Unternehmens-IT, Fernwartungssystemen oder Cloud-Plattformen verbunden. Dadurch entstehen zusätzliche Schnittstellen, die potenziell als Angriffsvektoren genutzt werden können [9]. Studien der Europäischen Agentur für Cybersicherheit zeigen, dass unzureichend gesicherte Remote-Zugänge und eine fehlende Netzwerksegmentierung zu den häufigsten Schwachstellen in urbanen Infrastrukturen gehören [10].

Hinzu kommt die mangelnde Transparenz gewachsener Systemumgebungen. Unterschiedliche Hersteller, nicht standardisierte Kommunikationsprotokolle und heterogene Komponenten erschweren eine vollständige Übersicht über vorhandene Assets und Kommunikationsbeziehungen. Ohne eine verlässliche Asset-Identifikation sind jedoch weder eine systematische Risikoanalyse noch eine wirksame Segmentierung möglich [7]. Dies stellt insbesondere in kommunalen Infrastrukturen mit historisch gewachsenen Architekturen eine große technische Herausforderung dar.

Zusammenfassend lassen sich die technologischen Herausforderungen auf drei zentrale Faktoren verdichten: veraltete oder nur eingeschränkt modernisierbare Systeme, Zielkonflikte zwischen Verfügbarkeit und Sicherheit sowie eine wachsende Angriffsfläche infolge zunehmender Vernetzung. Auf Basis dieser Rahmenbedingungen ergeben sich weitere organisatorische und strukturelle Fragestellungen im Bereich der OT-Security in Smart-City-Infrastrukturen.

Neben technologischen Faktoren sind es vor allem organisatorische Rahmenbedingungen, die eine zentrale Herausforderung für die OT-Security in Smart-City-Infrastrukturen darstellen. Anders als in klassischen Industrieunternehmen sind urbane Infrastrukturen häufig durch komplexe Strukturen

gekennzeichnet. Kommunen, Stadtwerke, private Dienstleister und externe Systemintegratoren teilen sich die Verantwortung und die Zuständigkeiten. Diese Fragmentierung erschwert die Entwicklung einer konsistenten Sicherheitsstrategie und führt oftmals zu unklaren Verantwortlichkeiten im Bereich der OT-Security [10].

Ein wesentliches Problem besteht in der fehlenden klaren Zuordnung der Sicherheitsverantwortung zwischen den Bereichen IT und OT. Während IT-Abteilungen typischerweise für die Informationssicherheit zuständig sind, liegen industrielle Steuerungssysteme häufig im Verantwortungsbereich technischer Betriebsabteilungen. Da die Prioritäten in beiden Bereichen unterschiedlich sind – etwa Verfügbarkeit und Prozessstabilität im OT-Bereich versus Daten- und Netzwerkschutz in der IT –, kann es zu Zielkonflikten kommen [11]. Ohne abgestimmte Governance-Strukturen bleibt eine einheitliche Sicherheitsarchitektur schwer durchzuführen.

Hinzu kommt der Fachkräftemangel im Bereich der industriellen Cybersicherheit. Die Sicherung von OT-Systemen erfordert interdisziplinäres Know-how, das sowohl Kenntnisse industrieller Prozesse als auch IT-Sicherheitskompetenz umfasst. Studien zeigen, dass kommunale Betreiber insbesondere häufig nur über begrenzte personelle Ressourcen für spezialisierte OT-Sicherheitsaufgaben verfügen [6]. Dies führt dazu, dass Sicherheitsmaßnahmen reaktiv statt strategisch geplant umgesetzt werden.

Ein weiterer organisatorischer Faktor betrifft das Risikomanagement. In vielen Infrastrukturbereichen wurde erst in den vergangenen Jahren damit begonnen, Cybersecurity systematisch in bestehende Managementprozesse zu integrieren. Internationale Leitlinien betonen jedoch, dass Cyber-Risiken kontinuierlich bewertet und in bestehende Sicherheits- und Notfallkonzepte eingebunden werden müssen. [12]. Fehlende oder unzureichend dokumentierte Prozesse zur Risikoidentifikation und Incident-Response können im Ernstfall zu verzögerten Reaktionen führen.

Schließlich ist auch die Sensibilisierung von Mitarbeitenden eine Herausforderung. Das technische Personal in Versorgungsunternehmen ist in der Regel vorrangig auf den sicheren Anlagenbetrieb fokussiert. Cybersecurity wird teilweise als zusätzliche Belastung wahrgenommen. Insbesondere, wenn Sicherheitsmaßnahmen als betriebshemmend empfunden werden. Ohne eine verankerte Sicherheitskultur bleiben technische Schutzmechanismen jedoch nur eingeschränkt wirksam [7].

Neben technologischen und organisatorischen Faktoren wird die OT-Security in Smart-City-Infrastrukturen maßgeblich durch regulatorische und strukturelle Rahmenbedingungen beeinflusst. Betreiber kritischer Infrastrukturen unterliegen zunehmend gesetzlichen Vorgaben, die Mindestanforderungen an Informationssicherheit und Risikomanagement definieren. Auf europäischer Ebene schafft insbesondere die NIS-Richtlinie (Richtlinie über die Netz- und Informationssicherheit) einen verbindlichen Rahmen zur Stärkung der Cybersicherheit kritischer Dienste [13]. Diese regulatorischen Anforderungen werden in nationales Recht überführt und verpflichten Betreiber dazu, angemessene technische und organisatorische Sicherheitsmaßnahmen umzusetzen.

Für industrielle Steuerungssysteme existieren darüber hinaus spezifische Normen und Standards. So definiert beispielsweise die Normenreihe IEC 62443 Anforderungen an sichere Architekturen, Risikobewertungen und Sicherheitsprozesse in industriellen Kommunikationsnetzen [8]. Sie verfolgt einen ganzheitlichen Ansatz, der sowohl Produktanforderungen als auch die Betreiberverantwortung berücksichtigt. Die Umsetzung solcher Standards ist jedoch insbesondere für kommunale Betreiber strukturell herausfordernd, da sie Investitionen in Technik, Personal und Dokumentationsprozesse erfordert.

Ein weiteres strukturelles Problem ergibt sich aus den unterschiedlichen Aufbauten kommunaler Infrastrukturen. Während große Energieversorger häufig über etablierte Sicherheitsabteilungen verfügen, sind kleinere Stadtwerke oder Verkehrsunternehmen organisatorisch und finanziell eingeschränkter aufgestellt. Studien zur Resilienz kritischer Infrastrukturen zeigen, dass das Sicherheitsniveau stark von der Größe, den Ressourcen und der organisatorischen Reife der jeweiligen Betreiber abhängt [6]. Dies hat eine fragmentierte Sicherheitslandschaft in urbanen Räumen zur Folge.

Beschaffungsprozesse und langfristige Investitionszyklen beeinflussen darüber hinaus die Sicherheitsarchitektur. Da öffentliche Vergabeverfahren häufig die Wirtschaftlichkeit priorisieren, werden Sicherheitsanforderungen nicht immer frühzeitig in Systemdesigns integriert. Gleichzeitig machen langfristige Vertragsbindungen mit Technologieanbietern eine flexible Anpassung an neue Bedrohungslagen schwer. [10]. Sicherheitsanforderungen müssen daher zunehmend bereits in den Phasen der Planung und Beschaffung berücksichtigt werden (Security by Design).

3. Methodisches Vorgehen

Die Fallstudie verfolgt das Ziel, sicherheitsrelevante Schwachstellen, Angriffsmuster und strukturelle Herausforderungen in OT-Systemen kritischer Smart-City-Infrastrukturen systematisch zu identifizieren. Durch die Analyse realer Vorfälle in den Bereichen Smart Grids, Wasser-/Abwassersysteme und Verkehrssysteme sollen domänenspezifische Besonderheiten sichtbar gemacht und zugleich übergreifende Muster herausgearbeitet werden. Die Fallstudie dient damit der theoriegeleiteten Untersuchung komplexer sozio-technischer Systeme, deren Verhalten und Verwundbarkeit nur im Kontext realer Ereignisse angemessen verstanden werden kann [18].

Ein Mehrfachfallstudien-Ansatz wird gewählt, weil er die Analyse mehrerer Fälle nach einem einheitlichen methodischen Raster erlaubt und dadurch die Vergleichbarkeit der Ergebnisse sicherstellt. Die Gegenüberstellung verschiedener Fälle unterstützt die Identifikation wiederkehrender Muster und erhöht die theoretische Verallgemeinerbarkeit der Erkenntnisse. Mehrere Fälle gelten als besonders geeignet, um robuste Schlussfolgerungen über komplexe technische und organisatorische Systeme zu ziehen, da sie sowohl Gemeinsamkeiten als auch Unterschiede sichtbar machen [19]. Die methodische Orientierung folgt damit den etablierten Standards der Fallstudienforschung.

Die gewählte Forschungsstrategie ist ein qualitatives, mehrfallbasiertes Forschungsdesign, das auf den Aufbau von Theorie aus Fallstudien ("building theory from case study research") abzielt [19,

20]. Dieses Design eignet sich insbesondere für Forschungsfelder, in denen vorhandene Theorien noch begrenzt oder fragmentiert sind und in denen komplexe, kontextabhängige Phänomene untersucht werden – wie dies bei OT-Security-Risiken in Smart-City-Infrastrukturen der Fall ist [18]. Anstatt Hypothesen a priori zu testen, werden theoretische Einsichten aus der detaillierten Analyse einzelner Fälle entwickelt und im Verlauf der Studie schrittweise verfeinert [19]. Die Kombination aus Within-Case-Analyse und Cross-Case-Vergleich erlaubt es, sowohl fallinterne Besonderheiten als auch übergreifende Muster in Angriffsvektoren, Schwachstellen und Gegenmaßnahmen sichtbar zu machen [20]. Auf diese Weise verfolgt die Arbeit eine analytische, nicht statistische Generalisierung, bei der aus konkreten Fällen generalisierbare Handlungsfelder für Betreiber kritischer Infrastrukturen abgeleitet werden [18].

Die Auswahl der Fälle erfolgt nach dem Prinzip der theoretischen Stichprobenziehung („theoretical, not random, sampling“), wie es im Rahmen des theorieaufbauenden Fallstudiendesigns empfohlen wird. Ziel ist es nicht, eine statistisch repräsentative Stichprobe aller OT-Sicherheitsvorfälle zu ziehen, sondern Fälle zu identifizieren, die für die Entwicklung und Schärfung theoretischer Konzepte besonders informationsreich sind. Im Sinne dieses Ansatzes werden Fälle bevorzugt, die entweder erwartete Muster in unterschiedlichen Kontexten replizieren oder bewusst kontrastierende Bedingungen aufweisen, um die Grenzen und Gültigkeit der entstehenden Theorie auszuloten. Die drei in dieser Arbeit untersuchten Vorfälle – der Angriff auf das ukrainische Stromnetz, der Oldsmar-Vorfall in einer Wasseraufbereitungsanlage und der Angriff auf die Notfallsirenen in Dallas – wurden daher nicht zufällig, sondern anhand fachlich-theoretischer Kriterien ausgewählt. Diese Form der Stichprobenziehung unterstützt eine analytische Verallgemeinerung der Ergebnisse auf ähnliche OT-basierte Smart-City-Infrastrukturen, ohne einen Anspruch auf statistische Repräsentativität zu erheben.

Die Auswahl der untersuchten Fälle erfolgt nicht zufällig, sondern auf Grundlage klar definierter fachlicher und methodischer Kriterien. Ziel ist es, solche Sicherheitsvorfälle auszuwählen, die einerseits einen hohen inhaltlichen Bezug zur Forschungsfrage aufweisen und andererseits eine belastbare vergleichende Analyse ermöglichen. Im Sinne der theoretischen Stichprobenziehung dient die Fallauswahl somit der gezielten Untersuchung informationsreicher und analytisch relevanter Fälle [18, 19]. Ein erstes zentrales Auswahlkriterium ist der OT-Bezug des jeweiligen Vorfalls. Berücksichtigt werden ausschließlich Fälle, in denen Operationstechnologie beziehungsweise industrielle oder prozessnahe Steuerungssysteme unmittelbar betroffen sind. Reine IT-Sicherheitsvorfälle ohne Bezug zu physischen Steuerungs- oder Überwachungsprozessen werden ausgeschlossen, da sie die spezifischen Herausforderungen der OT-Security nicht hinreichend abbilden [3, 25].

Ein zweites Kriterium ist der direkte physische Prozessbezug. In die Analyse einbezogen werden nur Vorfälle, bei denen digitale Angriffe unmittelbar auf physische Prozesse, Anlagenzustände oder sicherheitsrelevante Steuerungsfunktionen einwirken konnten. Dieses Kriterium ist zentral, da die Arbeit gezielt jene Smart-City-Infrastrukturen untersucht, in denen Cyberangriffe nicht nur

digitale, sondern auch operative und gesellschaftlich relevante physische Auswirkungen entfalten können.

Drittens müssen die ausgewählten Fälle einer kritischen Smart-City-Infrastruktur zugeordnet werden können. Dies betrifft im Rahmen der vorliegenden Arbeit Infrastrukturen der Energieversorgung, Wasser- und Abwassersysteme sowie urbane Warn- und Leitsysteme mit öffentlicher Schutzfunktion. Die Zugehörigkeit zu kritischen Infrastrukturen ist deshalb relevant, weil hier ein erhöhtes Schutzbedürfnis besteht und Sicherheitsvorfälle potenziell erhebliche Folgen für Versorgungssicherheit, öffentliche Ordnung oder gesellschaftliches Vertrauen nach sich ziehen können [6].

Ein weiteres Auswahlkriterium ist die ausreichende Dokumentation der Vorfälle. Analysiert werden nur solche Fälle, für die belastbare Primär- oder Sekundärquellen vorliegen, etwa in Form technischer Berichte, offizieller Stellungnahmen, behördlicher Advisories oder fachlich anerkannter Analysen. Dieses Kriterium ist notwendig, um den Vorfallverlauf, die Schwachstellen, die Auswirkungen sowie die Reaktionen nachvollziehbar rekonstruieren zu können. Eine unzureichende Dokumentationslage würde die Reliabilität und Validität der Fallanalyse erheblich einschränken [22, 23].

Fünftens wird auf sektorale Heterogenität geachtet. Die Fallauswahl soll unterschiedliche Infrastrukturbereiche abdecken, um nicht nur sektorspezifische Besonderheiten, sondern auch fallübergreifende Gemeinsamkeiten identifizieren zu können. Die Auswahl eines Falles aus dem Energiesektor, eines aus der Wasserinfrastruktur sowie eines aus einem urbanen Warn- und Steuerungssystem ermöglicht es, sowohl infrastrukturspezifische Unterschiede als auch gemeinsame Muster der OT-Verwundbarkeit sichtbar zu machen.

Schließlich ist die theoretische Relevanz für das Pattern-Matching ein wesentliches Auswahlkriterium. Die Fälle werden so ausgewählt, dass sie entweder erwartbare Muster in unterschiedlichen Kontexten bestätigen oder kontrastierende Ausprägungen desselben Grundproblems sichtbar machen. Auf diese Weise wird es möglich, die in der Literatur beschriebenen Verwundbarkeitsstrukturen von OT-Systemen mit den empirisch beobachteten Fallmustern systematisch abzugleichen [18,20]. Die ausgewählten Fälle sind daher nicht nur praktisch relevant, sondern auch theoretisch geeignet, um wiederkehrende Angriffsvektoren, strukturelle Schwachstellen und generalisierbare Handlungsfelder herauszuarbeiten.

Insgesamt stellt die Kombination dieser Auswahlkriterien sicher, dass die Fallstudien sowohl thematisch einschlägig als auch methodisch geeignet sind, um die Forschungsfrage der vorliegenden Arbeit belastbar zu beantworten. Die Fallauswahl folgt damit einer theoriegeleiteten und zugleich forschungspraktisch nachvollziehbaren Logik.

Die vorliegende Arbeit basiert auf einer qualitativen Analyse sekundärer Datenquellen, die dokumentierte Sicherheitsvorfälle im Bereich der OT-Security in kritischen Smart-City-Infrastrukturen beschreiben. Der Einsatz sekundärer Daten ist insbesondere in der Sicherheitsforschung etabliert, da reale Cybervorfälle häufig nicht primär erhoben werden können

und stattdessen auf veröffentlichte Analysen und Incident Reports zurückgegriffen werden muss [19, 22].

Die Datengrundlage umfasst technische Berichte, offizielle Untersuchungen sowie Analysen von Fachorganisationen wie dem Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), der European Union Agency for Cybersecurity (ENISA) sowie weiteren sicherheitsrelevanten Institutionen, die detaillierte Informationen zu Angriffsverläufen, Schwachstellen und Auswirkungen bereitstellen [10, 25].

Zur Sicherstellung der Validität der Analyse wird ein Ansatz der methodischen Triangulation verfolgt, bei dem mehrere unabhängige Quellen pro Fall herangezogen und miteinander abgeglichen werden. Dieser Ansatz dient dazu, Verzerrungen einzelner Berichte zu reduzieren und ein möglichst vollständiges Bild der jeweiligen Sicherheitsvorfälle zu rekonstruieren [19, 23].

Die Auswahl der konkreten Fallstudien basiert auf einer gezielten Zusammenstellung dokumentierter Vorfälle aus unterschiedlichen Infrastrukturbereichen, die jeweils spezifische Angriffsformen und Schwachstellen repräsentieren. Die betrachteten Fälle umfassen Sicherheitsvorfälle aus den Bereichen Energieversorgung, Wasserinfrastruktur sowie verkehrsbezogene Steuerungssysteme und ermöglichen damit eine sektorübergreifende Analyse von OT-Sicherheitsrisiken [16, 18].

Durch die Kombination dieser heterogenen Datenquellen wird eine vergleichende Analyse ermöglicht, die sowohl fallbezogene Besonderheiten als auch übergreifende Muster identifizieren kann. Gleichzeitig ist zu berücksichtigen, dass die Datengrundlage auf öffentlich zugänglichen Informationen basiert und somit potenziell unvollständig sein kann, da nicht alle Details von Sicherheitsvorfällen veröffentlicht werden [20].

Insgesamt ermöglicht die gewählte Datengrundlage eine systematische und nachvollziehbare Analyse realer OT-Sicherheitsvorfälle und bildet damit die Grundlage für die anschließende fallübergreifende Auswertung und Ableitung von Handlungsfeldern.

Um eine systematische Vergleichbarkeit der heterogenen Sicherheitsvorfälle zu gewährleisten, folgt die Analyse einem standardisierten Analyserahmen. Dieser Rahmen stellt sicher, dass die Untersuchung über alle Einzelfälle hinweg konsistent bleibt und die Grundlage für die spätere Cross-Case-Analyse bildet [18, 19].

Die Auswertung der Dokumente erfolgt mittels eines deduktiv hergeleiteten Kategoriensystems, das auf der qualitativen Inhaltsanalyse nach [15] basiert. Das Raster umfasst sieben Kernkategorien, die auf jeden Fall gleichermaßen angewendet werden:

12. Kontext und Systembeschreibung: Identifikation der betroffenen Infrastruktur, der Betreiberstruktur sowie der spezifischen OT-Architektur und der genutzten Kommunikationswege [18].
13. Angriffsvektor und Ablauf: Rekonstruktion des zeitlichen Ablaufs, beginnend beim initialen Zugang (Initial Access) über die seitliche Ausbreitung (Lateral Movement) bis hin zur Manipulation der physischen Prozesse.

14. Technische Schwachstellen: Systematische Erfassung technischer Defizite, wie mangelnde Netzwerksegmentierung, unsichere Protokolle, unzureichende Authentifizierung oder fehlendes Patch-Management.
15. Organisatorische Schwachstellen: Analyse prozessualer Mängel, insbesondere in den Bereichen Rollenverteilung, Sicherheitsmonitoring und Notfallmanagement.
16. Auswirkungen: Dokumentation der technischen, operativen und gesellschaftlichen Konsequenzen des Vorfalls (z. B. Versorgungsausfälle oder Sicherheitsrisiken für die Bevölkerung).
17. Reaktion und Incident Response: Untersuchung der eingeleiteten Sofortmaßnahmen, des Wiederherstellungsprozesses sowie der Qualität der forensischen Aufarbeitung.
18. Lessons Learned und Handlungsfelder: Ableitung von präventiven Maßnahmen auf technischer, organisatorischer und strategischer Ebene für zukünftige Smart-City-Infrastrukturen.

Der Analyseprozess folgt einem strengen, mehrstufigen Protokoll, um die Reliabilität der Ergebnisse nach [21] sicherzustellen:

19. Materialaufbereitung und Sichtung: Alle im Rahmen der Datenerhebung nach [22] identifizierten Dokumente werden vollständig gesichtet und chronologisch geordnet.
20. Kodierung: Textstellen, die für die oben genannten sieben Kategorien relevant sind, werden systematisch extrahiert. Dabei wird primär deduktiv (nach dem Raster) vorgegangen, wobei das System bei Bedarf induktiv um fallspezifische Unterkategorien ergänzt wird, um domänenspezifische Besonderheiten (z. B. Funkprotokolle im Verkehrssektor) zu erfassen [15].
21. Erstellung strukturierter Fallbeschreibungen: Für jeden der drei Fälle wird eine detaillierte Einzelanalyse verfasst, die alle Kategorien des Rasters abdeckt. Zentrale Aussagen werden dabei stets durch Primär- oder Sekundärquellen belegt.
22. Analytische Verdichtung: Die Ergebnisse werden innerhalb der Kategorien zusammengefasst, um die wesentlichen Schwachstellen und Muster pro Einzelfall klar herauszuarbeiten. Dies bildet die notwendige Vorstufe für die anschließende Synthese in der Cross-Case-Analyse nach [19].

4. Fallstudienanalyse

4.1 Fall 1: Smart Grids – Ukraine Power Grid Attack (2015)

Kontext und Systembeschreibung Der Sicherheitsvorfall vom 23. Dezember 2015 gilt als einer der ersten öffentlich umfassend dokumentierten Cyberangriffe, bei denen durch die Kompromittierung von OT-Systemen ein realer Stromausfall verursacht wurde. Betroffen waren mehrere regionale Energieversorger in der Ukraine, deren Verteilnetze über industrielle Steuerungs- und Leitsysteme betrieben wurden. Die angegriffene Infrastruktur lässt sich dem Bereich kritischer Smart-Grid-Systeme zuordnen, da digitale Leit- und Fernwirktechnik eingesetzt wurde, um Schaltvorgänge, Netzüberwachung und Betriebsführung innerhalb des

Stromverteilnetzes zu steuern [3, 4, 9, 18]. Die öffentlich verfügbaren Berichte beschreiben eine Umgebung, in der klassische Office-IT, betriebliche Netzwerke und OT-nahe Steuerungssysteme funktional miteinander verbunden waren, wodurch die Voraussetzungen für eine Bewegung der Angreifer aus der IT- in die OT-Ebene geschaffen wurden [3, 25]. CISA beschreibt den Vorfall als „unscheduled power outages impacting a large number of customers“ am 23. Dezember 2015; SANS wertet ihn als koordinierten Angriff auf mehrere ukrainische Stromversorger.

Angriffsvektor und Ablauf Nach der in der Literatur und in technischen Berichten rekonstruierten Angriffskette begann der Vorfall mit einer initialen Kompromittierung der Unternehmens-IT durch Spear-Phishing. Anschließend etablierten die Angreifer Persistenz, bewegten sich lateral innerhalb der Netze und verschafften sich Zugriff auf Systeme mit Bezug zur Netzsteuerung. In der finalen Phase wurden legitime Fernsteuerungsfunktionen missbraucht, um Umspannwerke aus der Ferne abzuschalten und damit die Stromversorgung in mehreren Regionen gezielt zu unterbrechen [3, 4, 18]. Der Angriff war damit nicht als opportunistische Störung, sondern als mehrstufige und zielgerichtete Operation strukturiert, bei der sowohl Kenntnisse über die IT-Landschaft als auch über betriebliche Abläufe der Stromverteilung vorausgesetzt werden mussten [7, 11]. Laut CISA und dem SANS/E-ISAC-Bericht begann die Kill Chain mit Spear-Phishing, führte über die Kompromittierung der IT-Umgebung bis zum Missbrauch von Fernzugriffen auf die SCADA-/Verteilnetzebene.

Technische Schwachstellen Die Fallanalyse zeigt mehrere technische Schwachstellen, die den Angriff ermöglichten oder erheblich begünstigten. Erstens deutet der Vorfall auf eine unzureichende Segmentierung zwischen Office-IT und betrieblichen Steuerungsumgebungen hin. Zweitens spielten Fernzugänge eine zentrale Rolle, da vorhandene Remote-Access-Möglichkeiten den Übergang in betriebsnahe Systeme erleichterten. Drittens verweist der Fall auf ein Umfeld, in dem Sichtbarkeit, Härtung und technische Überwachung der

OT-Kommunikation nicht in hinreichendem Maß etabliert waren, sodass die Angreifer über einen längeren Zeitraum unentdeckt agieren konnten [3, 11, 25, 27]. Hinzu kommt, dass OT-Umgebungen aufgrund langer Lebenszyklen, proprietärer Protokolle und eingeschränkter Patchbarkeit strukturell schwerer abzusichern sind als klassische IT-Systeme, was die technische Resilienz gegenüber gezielten Angriffen zusätzlich reduziert [4, 8]. Sowohl CISA als auch der SANS-Bericht heben Defizite bei Netzwerksegmentierung, Fernzugriffen und OT-spezifischer Sichtbarkeit als zentrale Lehren aus dem Vorfall hervor.

Organisatorische Schwachstellen Neben den technischen Faktoren offenbart der Fall auch deutliche organisatorische Schwächen. Die Angriffsdauer und der koordinierte Ablauf legen nahe, dass Prozesse zur Früherkennung, Eskalation und Reaktion auf sicherheitsrelevante Auffälligkeiten nicht ausreichend wirksam waren. Ebenso wird deutlich, dass in hybriden IT-/OT-Umgebungen unklare Verantwortungsgrenzen zwischen IT-Sicherheit, Netzbetrieb und technischer Betriebsführung die Reaktionsfähigkeit beeinträchtigen können [7,10,12]. Der Ukraine-Fall zeigt damit exemplarisch, dass OT-Security nicht ausschließlich eine technische Frage ist, sondern maßgeblich von Governance-Strukturen, Incident-Response-Prozessen und

einer abgestimmten Sicherheitsorganisation abhängt [6, 14]. Die öffentlichen Analysen betonen, dass die Angreifer koordiniert vorgingen und die betroffenen Organisationen sowohl technisch als auch organisatorisch unter Druck setzten; das spricht für Schwächen in Detection, Vorbereitung und Krisenreaktion.

Auswirkungen Die Auswirkungen des Vorfalls waren sowohl operativ als auch gesellschaftlich erheblich. Durch die Abschaltung betroffener Systeme kam es zu Stromausfällen, von denen eine große Zahl an Endverbrauchern betroffen war. Der Fall macht damit deutlich, dass Cyberangriffe auf OT-Systeme unmittelbare physische Konsequenzen entfalten können und sich nicht auf Datenverluste oder IT-Störungen beschränken [3, 4, 6]. Darüber hinaus hatte der Vorfall eine hohe symbolische und strategische Wirkung, da er die Verwundbarkeit digitalisierter Energieinfrastrukturen international sichtbar machte und die Diskussion über Smart-Grid-Sicherheit nachhaltig beeinflusste [9, 26]. CISA berichtet von einer großen Zahl betroffener Kunden; der SANS/E-ISAC-Bericht nennt rund 225.000 betroffene Haushalte.

Reaktion und Incident Response Die Reaktion auf den Vorfall zeigt, dass betriebliche Resilienz in OT-Umgebungen nicht allein von Präventionsmaßnahmen abhängt, sondern auch von der Fähigkeit, im Störfall kontrolliert in manuelle oder alternative Betriebsmodi überzugehen. In der Fachliteratur wird der Ukraine-Fall häufig als Beispiel dafür angeführt, dass manuelle Schalthandlungen und betriebliche Redundanzen eine wichtige Rolle bei der Wiederherstellung kritischer Funktionen spielen können [3, 11, 25]. Gleichzeitig verdeutlicht der Fall die Bedeutung forensischer Aufarbeitung und sektorübergreifender Wissensweitergabe, da erst durch die technische Analyse des Angriffspfades belastbare Lehren für andere Betreiber kritischer Infrastrukturen gezogen werden konnten [18, 19]. CISA und SANS stellen den Vorfall ausdrücklich als Lernfall für verbesserte Detektion, Segmentierung, Notfallplanung und Wiederherstellung dar.

Lessons Learned und Handlungsfelder Aus dem Fall lassen sich mehrere zentrale Handlungsfelder für die Absicherung von Smart Grids ableiten. Erstens ist eine konsequente Trennung von IT- und OT-Netzen durch Segmentierung und Zonenbildung erforderlich, um laterale Bewegungen in Richtung betrieblicher Steuerungssysteme zu erschweren [3, 8, 27]. Zweitens müssen Fernzugriffe auf OT-nahe Systeme strikt kontrolliert, gehärtet und kontinuierlich überwacht werden, da sie im vorliegenden Fall eine wesentliche Rolle für die operative Umsetzung des Angriffs spielten [25, 26]. Drittens zeigt der Vorfall die Notwendigkeit eines OT-spezifischen Monitorings, das nicht nur klassische IT-Indikatoren, sondern auch ungewöhnliche Steuerungs- und Kommunikationsmuster innerhalb industrieller Netzwerke erfassen kann [7, 11]. Viertens sind organisatorische Maßnahmen wie klare Zuständigkeiten, abgestimmte Incident-Response-Prozesse und regelmäßige Übungen essenziell, um im Ereignisfall schnell und koordiniert reagieren zu können [6, 12]. Insgesamt verdeutlicht der Ukraine-Fall, dass die wesentlichen Risiken nicht aus einer einzelnen Schwachstelle resultierten, sondern aus dem Zusammenwirken technischer Exponiertheit, unzureichender Segmentierung, angreifbarer Fernzugänge und organisatorischer Defizite. Diese Kombination macht den Fall zu einem besonders geeigneten

Referenzfall für die Analyse von OT-Security in Smart-Grid-Infrastrukturen. Die offiziellen und fachlichen Auswertungen ziehen sehr ähnliche Lehren: stärkere Netzwerksegmentierung, bessere Überwachung, Härtung von Remote Access und belastbare Notfallprozesse.

4.2 Fall 2: Wasser-/Abwassersysteme – Oldsmar Water Treatment Plant Attack (2021)

Kontext und Systembeschreibung Der Vorfall im Wasserwerk der Stadt Oldsmar in Florida im Februar 2021 stellt ein prägnantes Beispiel für die Verwundbarkeit kommunaler Wasserinfrastrukturen gegenüber Cyberangriffen dar. Betroffen war eine Anlage zur Wasseraufbereitung, in der digitale Steuerungs- und Überwachungssysteme eingesetzt wurden, um chemische Prozesse, Betriebszustände und Eingriffe durch das Bedienpersonal zu kontrollieren. Damit ist der Fall dem Bereich kritischer Wasser- und Abwassersysteme mit direktem physischem Prozessbezug zuzuordnen, da Änderungen an den Steuerungsparametern unmittelbare Auswirkungen auf die Wasserqualität und damit auf die öffentliche Versorgungssicherheit haben können [3, 11, 25]. Aus den öffentlich bekannten Informationen geht hervor, dass die Anlage über Human-Machine-Interfaces (HMI), Windows-basierte Bedienrechner und Fernzugriffsmöglichkeiten verfügte, wodurch eine digitale Interaktion mit prozessrelevanten Parametern möglich war [3, 10].

Angriffsvektor und Ablauf Der Angriff wurde bekannt, nachdem ein Anlagenbediener beobachtete, dass sich der Mauszeiger auf dem Bildschirm eines Bedienrechners eigenständig bewegte und Einstellungen innerhalb des Systems verändert wurden. Im Zuge des Vorfalls wurde der Wert für die Dosierung von Natriumhydroxid, das in Wasseraufbereitungsprozessen zur Regulierung des pH-Werts verwendet wird, in kurzer Zeit massiv erhöht. Nach den verfügbaren Berichten wurde hierfür ein bestehender Fernzugriff auf das System missbraucht, sodass der Angriff nicht über eine komplexe mehrstufige laterale Bewegung, sondern über den direkten Zugriff auf ein prozessnahes System erfolgte [7,11,25]. Der Fall zeigt damit exemplarisch, dass in kleineren kommunalen Infrastrukturen bereits vergleichsweise einfache Angriffsvektoren erhebliche Risiken verursachen können, wenn ein direkter Zugriff auf HMI- oder SCADA-nahe Bedienoberflächen besteht [3, 26].

Technische Schwachstellen Die Analyse des Vorfalls verweist auf mehrere technische Schwachstellen, die den Angriff ermöglichten oder erheblich begünstigten. Zunächst spielte die Existenz eines extern erreichbaren Fernzugangs eine zentrale Rolle, da dieser offenbar die unmittelbare Interaktion mit einem prozessrelevanten Bedienrechner ermöglichte [25, 27]. Darüber hinaus deutet der Fall auf eine unzureichende Absicherung des Remote Access hin, insbesondere im Hinblick auf Authentifizierung, Zugriffsbeschränkung und Überwachung aktiver Sitzungen [7, 8]. Ferner wird in der öffentlichen Diskussion des Falls regelmäßig auf eine geringe Segmentierung zwischen administrativen und operativen Systembereichen sowie auf den Einsatz veralteter Betriebssystemumgebungen verwiesen, was die technische Resilienz gegenüber einem unautorisierten Zugriff zusätzlich reduziert haben dürfte [3, 4, 11]. Der Fall macht damit deutlich, dass die Kombination aus externem Fernzugriff, unzureichender Härtung und begrenzter OT-

spezifischer Schutzarchitektur ein erhebliches Risiko für kommunale Wasserinfrastrukturen darstellt [10, 25].

Organisatorische Schwachstellen Neben den technischen Defiziten offenbart der Vorfall auch deutliche organisatorische Schwächen. Der Umstand, dass ein sicherheitskritischer Eingriff überhaupt über einen Fernzugang erfolgen konnte, verweist auf Defizite in der Governance des Zugriffsmanagements sowie in der organisatorischen Kontrolle privilegierter Zugänge [7, 12]. Zudem deutet der Fall darauf hin, dass in kleineren kommunalen Einrichtungen Sicherheitsmaßnahmen häufig weniger formalisiert, personell begrenzt und stärker betriebspraktisch als strategisch ausgestaltet sind [6, 10]. Gleichzeitig zeigt der Vorfall, wie stark die Entdeckung eines Angriffs in solchen Umgebungen von der Aufmerksamkeit einzelner Bedienpersonen abhängen kann. Dass die Manipulation der chemischen Dosierung durch einen Mitarbeiter bemerkt und rückgängig gemacht wurde, spricht dafür, dass technische Detektions- und Alarmsysteme allein entweder nicht vorhanden oder nicht hinreichend wirksam waren [11,12]. Daraus ergibt sich, dass organisatorische Vorkehrungen wie klare Zuständigkeiten, kontrollierte Fernzugriffsprozesse, Schulung des Personals und definierte Reaktionsabläufe eine zentrale Rolle für die Sicherheit von Wasserinfrastrukturen spielen [14, 16].

Auswirkungen Im konkreten Fall konnte eine tatsächliche Schädigung der Trinkwasserversorgung verhindert werden, da die Veränderung des Natriumhydroxid-Werts rechtzeitig erkannt und zurückgesetzt wurde. Gleichwohl war das potenzielle Schadensausmaß erheblich, da eine fehlerhafte chemische Dosierung in Wasseraufbereitungsanlagen direkte Folgen für die Wasserqualität und damit für die Gesundheit der Bevölkerung haben kann [3, 25]. Der Vorfall verdeutlicht damit in besonderer Weise, dass Cyberangriffe auf Wasserinfrastrukturen nicht nur betriebliche oder technische Störungen verursachen, sondern unmittelbar in sensible physische Versorgungsprozesse eingreifen können [6, 11]. Darüber hinaus hatte der Fall eine hohe mediale und politische Wirkung, da er exemplarisch sichtbar machte, wie verletzlich kommunale Infrastrukturen mit begrenzten Ressourcen gegenüber Cyberbedrohungen sein können [10].

Reaktion und Incident Response Die Reaktion auf den Vorfall bestand in der unmittelbaren Rücknahme der manipulierten Werte durch das Bedienpersonal sowie in nachgelagerten Prüfungen der Sicherheitslage und der Fernzugriffsmöglichkeiten. Aus analytischer Sicht zeigt der Fall, dass die unmittelbare Betriebsreaktion wirksam war, die eigentliche Resilienz jedoch stark von menschlicher Beobachtung und manueller Intervention abhing [7, 11]. Dies ist aus Sicht der OT-Security ambivalent: Einerseits konnte durch das Eingreifen des Personals ein physischer Schaden verhindert werden, andererseits legt der Fall offen, dass präventive technische und organisatorische Kontrollmechanismen nicht ausreichend waren, um den Angriff frühzeitig zu verhindern oder automatisch zu unterbinden [3, 12]. Für die Incident Response in Wasserinfrastrukturen lässt sich daraus ableiten, dass technische Überwachung, geregelte Fernzugriffsprozesse und klar definierte Eskalationsmechanismen eng aufeinander abgestimmt sein müssen [25, 27].

Lessons Learned und Handlungsfelder Aus dem Oldsmar-Fall lassen sich mehrere zentrale Handlungsfelder für die Absicherung kommunaler Wasser- und Abwassersysteme ableiten.

Erstens muss der Fernzugriff auf prozessnahe Systeme konsequent minimiert, technisch gehärtet und organisatorisch streng kontrolliert werden, da gerade in kleinen und mittleren Infrastrukturen externe Zugänge ein besonders kritischer Angriffsvektor sind [10, 25, 27]. Zweitens ist eine stärkere Segmentierung zwischen Office-IT, administrativen Systemen und OT-nahen Bedien- und Steuerungssystemen erforderlich, um direkte Eingriffe in physische Prozesse zu erschweren [3, 8]. Drittens zeigt der Fall die Notwendigkeit eines OT-spezifischen Monitorings, das ungewöhnliche Zugriffe und sicherheitskritische Änderungen an Prozessparametern frühzeitig erkennt [7, 11]. Viertens sind organisatorische Maßnahmen von besonderer Bedeutung, insbesondere die klare Regelung privilegierter Zugriffe, die Sensibilisierung des Bedienpersonals sowie die Etablierung belastbarer Incident-Response- und Notfallprozesse [6, 12]. Insgesamt ist der Oldsmar-Fall wissenschaftlich besonders wertvoll, weil er zeigt, dass erhebliche Gefährdungen physischer Prozesse nicht zwingend hochkomplexe Angriffsketten voraussetzen, sondern bereits aus vergleichsweise einfach ausnutzbaren Fernzugriffs- und Organisationsschwächen resultieren können. Damit eignet sich der Fall in besonderer Weise für die spätere Cross-Case-Analyse, da er ein Gegenbeispiel zu hochkomplexen Angriffen wie im Ukraine-Fall darstellt und gleichzeitig ähnliche Grundmuster der OT-Verwundbarkeit erkennen lässt.

4.3 Fall 3: Intelligente Verkehrsleitsysteme – Dallas Emergency Siren Hack (2017)

Kontext und Systembeschreibung Der Vorfall um das Outdoor-Warning-System der Stadt Dallas im April 2017 stellt ein relevantes Beispiel für die Verwundbarkeit urbaner Warn- und Steuerungssysteme dar, die im weiteren Sinne intelligenten verkehrsnahen bzw. sicherheitskritischen Leit- und Alarmsystemen zugeordnet werden können. Bei dem betroffenen System handelte es sich um ein stadtweites Netz von 156 Außensirenen, das zur Warnung der Bevölkerung vor Gefahrenlagen wie Tornados oder anderen Notfällen eingesetzt wird. Solche Systeme besitzen zwar nicht die gleiche prozessuale Logik wie klassische SCADA-Systeme in Energie- oder Wasserinfrastrukturen, weisen jedoch ebenfalls einen klaren OT-Bezug auf, da digitale bzw. funkbasierte Steuerungsbefehle unmittelbar physische Warnsignale im urbanen Raum auslösen [3, 4, 7]. Für Dallas ist dokumentiert, dass das Outdoor Warning System aus 156 Sirenen besteht und zur Warnung von Personen im Freien genutzt wird.

Angriffsvektor und Ablauf Der Vorfall ereignete sich am 7. April 2017, als sämtliche 156 Sirenen der Stadt Dallas ohne tatsächliche Gefahrenlage aktiviert wurden und mehrfach Alarm auslösten. Nach den öffentlichen Angaben der Stadt sowie der Berichterstattung wurde die Auslösung nicht durch einen klassischen Einbruch in ein IT-System verursacht, sondern durch die Übertragung bzw. Nachahmung des Funksignals, mit dem die Sirenen angesteuert werden. Der Angriff basierte somit auf einem externen Funkangriff beziehungsweise auf einer Art Signal-Spoofing oder Replay-Mechanismus und nicht auf einer kompromittierten Office-IT oder auf einer typischen lateralen Bewegung innerhalb digitaler Netze [7, 11]. Gerade dieser Ablauf macht den Fall analytisch besonders interessant, da er zeigt, dass OT-Sicherheitsprobleme in Smart-City-Infrastrukturen nicht zwingend aus der IT/OT-Konvergenz entstehen müssen, sondern auch aus unzureichend abgesicherten funkbasierten Steuerungsarchitekturen resultieren können. Dallas erklärte offiziell,

dass eine „intrusion“ die Sirenen auslöste; Stadtvertreter und Berichte beschrieben später, dass die Auslösung über ein nachgeahmtes bzw. gespooftes Radiosignal erfolgte.

Technische Schwachstellen Die Analyse des Vorfalls weist auf mehrere technische Schwachstellen hin. Zentrale Bedeutung hatte zunächst die funkbasierte Steuerung des Systems. Wenn Aktivierungssignale nicht hinreichend gegen Nachahmung, Replay oder unautorisierte Aussendung geschützt sind, kann bereits die Kenntnis oder Rekonstruktion der entsprechenden Steuerlogik zur unbefugten Auslösung physischer Warnsysteme führen [4, 7]. Im Dallas-Fall wurde in der öffentlichen Diskussion insbesondere auf Defizite bei Verschlüsselung, Authentifizierung und Signalhärtung verwiesen. Dadurch entstand eine Situation, in der das System zwar funktional einsatzfähig war, seine Kommunikationssicherheit jedoch nicht ausreichend gegen einen externen Angreifer abgesichert war [8, 11]. Der Fall illustriert damit eine OT-spezifische Schwachstelle, die sich von den zuvor betrachteten Fällen unterscheidet: Nicht der Missbrauch eines Remote-Zugangs oder die Bewegung durch ein hybrides Netz stand im Mittelpunkt, sondern die Verwundbarkeit eines dezentralen, funkgesteuerten Warnsystems auf Protokoll- und Kommunikationsebene. Berichte über den Vorfall nennen das Funksignal selbst als Angriffsweg; Dallas beschloss unmittelbar Sicherheitsverbesserungen und sprach von zusätzlichen Schutzmaßnahmen, einschließlich stärkerer Absicherung des Systems.

Organisatorische Schwachstellen Neben den technischen Schwächen offenbart der Vorfall auch organisatorische Defizite. Zum einen zeigt sich, dass die Sicherheitsbewertung eines solchen Systems offenbar die Möglichkeit eines externen Funkangriffs nicht in ausreichendem Maße berücksichtigt hatte. Zum anderen verweist der Vorfall auf Defizite in der Vorbereitung auf Fehl- oder Falschauslösungen großflächiger Warnsysteme, insbesondere im Hinblick auf Kommunikations- und Reaktionsprozesse gegenüber Bevölkerung, Leitstellen und Notrufdiensten [6, 12]. Der Angriff führte nicht nur zu einer unautorisierten Auslösung der Sirenen, sondern auch zu einer erheblichen Belastung des Notrufsystems, da zahlreiche Bürgerinnen und Bürger aufgrund des Fehlalarms den Notruf kontaktierten. Dies verdeutlicht, dass organisatorische Resilienz in solchen Infrastrukturen nicht allein aus der technischen Sicherung des Ausgangssystems besteht, sondern auch die Vorbereitung angrenzender Krisen- und Kommunikationsprozesse einschließen muss [7, 10]. Medienberichte und Analysen hielten fest, dass die Sirenen wiederholt auslösten und die 911-Leitungen stark belastet wurden.

Auswirkungen Die unmittelbaren Auswirkungen des Vorfalls bestanden in einer großflächigen Fehlalarmierung der Bevölkerung, einer erheblichen Irritation im Stadtgebiet

sowie in der Überlastung beziehungsweise starken Beanspruchung der Notrufinfrastruktur. Anders als im Ukraine- oder Oldsmar-Fall standen hier keine direkten Schäden an Energie- oder Wasserprozessen im Vordergrund, jedoch war die gesellschaftliche Wirkung des Angriffs erheblich. Die unautorisierte Aktivierung eines stadtweiten Warnsystems untergräbt das Vertrauen in die Verlässlichkeit öffentlicher Sicherheitsinfrastrukturen und kann im Ernstfall dazu führen, dass echte Warnungen weniger ernst genommen werden [6, 7]. Damit zeigt der Dallas-Fall, dass OT-Sicherheitsvorfälle auch dann erhebliche gesellschaftliche und sicherheitsrelevante Folgen

entfalten können, wenn kein klassischer Versorgungsprozess beeinträchtigt wird. Mehrere Berichte nennen 156 ausgelöste Sirenen, wiederholte Alarmzyklen und eine hohe Zahl von Notrufen als zentrale Folgen des Vorfalls.

Reaktion und Incident Response Die Reaktion der Stadt Dallas bestand kurzfristig in der Deaktivierung bzw. Unterbrechung des Sirenensystems, um die Falschauslösung zu stoppen, sowie in nachgelagerten technischen und administrativen Maßnahmen zur Härtung des Systems. Aus analytischer Perspektive zeigt der Vorfall, dass die Incident Response zwar letztlich wirksam war, jedoch unter Echtzeitbedingungen offenbar nur eingeschränkte Möglichkeiten bestanden, die unautorisierten Signale sofort selektiv zu unterbinden [11, 12]. Dies verweist auf einen wichtigen Aspekt OT-bezogener Resilienz: Nicht nur die Prävention, sondern auch die Möglichkeit einer kontrollierten Abschaltung, der schnellen Wiederherstellung sowie der robusten Krisenkommunikation muss bereits im Systemdesign vorgesehen werden [3, 27]. Dallas beschloss kurz nach dem Ereignis Notfallmaßnahmen und zusätzliche finanzielle Mittel für Sicherheitsverbesserungen am Sirenensystem.

Lessons Learned und Handlungsfelder Aus dem Dallas-Fall lassen sich mehrere zentrale Handlungsfelder für die Absicherung funkbasierter urbaner Warn- und Leitinfrastrukturen ableiten. Erstens müssen drahtlose Steuerungsprotokolle und Aktivierungssignale konsequent gegen Spoofing, Replay und unautorisierte Übertragung abgesichert werden, etwa durch robuste Authentifizierung, stärkere kryptographische Verfahren und systematische Härtung der Kommunikationsprotokolle [7, 8]. Zweitens zeigt der Fall die Bedeutung einer sicherheitsorientierten Architekturprüfung auch für solche Systeme, die nicht klassisch als

5. Cross-Case-Analyse und fallübergreifende Befunde

Die drei untersuchten Fälle unterscheiden sich hinsichtlich Sektor, technischer Architektur und konkretem Angriffsvektor, weisen jedoch zugleich mehrere wiederkehrende Muster auf. Während der Angriff auf das ukrainische Stromnetz durch eine mehrstufige Kompromittierung von IT- und OT-Systemen gekennzeichnet war, beruhte der Oldsmar-Vorfall auf einem direkten Missbrauch eines bestehenden Fernzugriffs auf ein prozessnahes System, und der Dallas-Fall auf der unautorisierten Auslösung eines funkbasierten Warnsystems über eine Schwäche im Kommunikationsweg [18,19,39–42]. Trotz dieser Unterschiede zeigen alle drei Fälle, dass nicht eine isolierte Einzelschwachstelle, sondern das Zusammenwirken technischer Exponiertheit, unzureichender Sicherheitskontrollen und organisatorischer Defizite den Angriffserfolg wesentlich begünstigt hat [3, 7, 25, 27]. Die Cross-Case-Betrachtung bestätigt damit die in der OT-Sicherheitsliteratur vertretene Annahme, dass Angriffe auf kritische Infrastrukturen typischerweise auf soziotechnischen Verwundbarkeitskonstellationen beruhen und nicht ausschließlich auf einzelnen technischen Fehlern [6, 10, 11]. Der Ukraine-Fall betraf einen koordinierten Angriff auf mehrere ukrainische Stromversorger mit physischen Stromausfällen; der Oldsmar-Fall beruhte auf unautorisiertem Zugriff auf das SCADA-System einer Wasseraufbereitungsanlage; der Dallas-Fall führte zur Fehlaktivierung aller 156 Außensirenen der Stadt.

Tabelle 1: Vergleichsmatrix der analysierten Sicherheitsvorfälle

Analysekategorie	Ukraine Power Grid (2015)	Oldsmar Water Plant (2021)	Dallas Siren Hack (2017)
Infrastrukturbereich	Smart Grid / Energieversorgung	Wasser- und Abwassersystem	Intelligentes Warn- / Verkehrsleitsystem
Systemtyp / OT-Bezug	SCADA, RTUs, Schutzrelais, Leitstellen	SCADA/HMI, Windows-basierte Bedienrechner, chemische Prozesssteuerung	Funkbasiertes Sirenensystem mit zentraler Auslösung
Primärer Angriffsvektor	Spear-Phishing, IT-Kompromittierung, laterale Bewegung in OT	Missbrauch eines bestehenden Fernzugriffs	Funkbasiertes Signal-Spoofing / Replay
Technische Schwachstellen	Fehlende Segmentierung, unsichere Fernzugänge, begrenzte OT-Sichtbarkeit	Ungesicherter Remote Access, geringe Segmentierung, veraltete Systeme	Fehlende/ungenügende Authentifizierung und Absicherung des Funksignals
Organisatorische Schwachstellen	Begrenzte Detection, unzureichende IT/OT-Koordination, Krisenvorbereitung	Schwaches Zugriffsmanagement, geringe Formalisierung, hohe Abhängigkeit vom Bedienpersonal	Unzureichende Berücksichtigung von Funkangriffen, Defizite in Alarm- und Kommunikationsprozessen
Auswirkungen	Stromausfälle, große Zahl betroffener Haushalte, hoher strategischer Effekt	Potenzielle Gefährdung der Trinkwasserqualität, hohe politische Aufmerksamkeit	Fehlalarmierung, Notrufüberlastung, Vertrauensverlust in Warninfrastruktur
Incident Response	Manuelle Wiederherstellung, forensische Aufarbeitung, sektorweite Lessons Learned	Manuelle Korrektur durch Bedienpersonal, Prüfung von Fernzugriffen	Abschaltung/Unterbrechung des Systems, nachgelagerte Härtung
Zentrale Handlungsfelder	Segmentierung, OT-Monitoring, Härtung von Remote Access, Notfallprozesse	Absicherung/-Minimierung von Remote Access, Monitoring, Governance	Absicherung funkbasierter Protokolle, Authentifizierung, Krisenkommunikation

5.1 Musterabgleich

Im Sinne des Pattern-Matching nach Yin dient die fallübergreifende Analyse dazu, empirisch beobachtete Muster mit theoretisch erwartbaren Verwundbarkeitsstrukturen von OT-Systemen abzugleichen [18]. Aus der Literatur waren insbesondere drei Muster erwartbar: erstens die sicherheitskritische Wirkung unzureichend kontrollierter Schnittstellen zwischen internen und externen Systemen, zweitens die begrenzte Übertragbarkeit klassischer IT-Sicherheitsmaßnahmen auf OT-Umgebungen und drittens die hohe Bedeutung organisatorischer Faktoren für Prävention und Reaktion [3, 10, 25, 27].

Das erste Muster bestätigt sich in allen drei Fällen deutlich, wenngleich in unterschiedlicher Ausprägung. Im Ukraine-Fall wurde der Übergang von der Office-IT in die OT-Umgebung durch unzureichend geschützte Netzgrenzen und operative Zugänge ermöglicht; im Oldsmar-Fall stellte ein bestehender Fernzugriff den direkten Einstieg in ein prozessnahes System dar; im Dallas-Fall war es kein klassischer Netzwerkzugang, sondern ein unzureichend geschützter funkbasierter Kommunikationskanal [39–42]. Die Fälle bestätigen damit das übergreifende Muster, dass OT-Angriffe häufig dort ansetzen, wo Steuerungssysteme über externe, administrative oder drahtlose Kommunikationswege erreichbar werden. CISA beschreibt für die Ukraine eine mehrstufige Kompromittierung mit resultierenden Stromausfällen; CISA/FBI/EPA beschreiben für Oldsmar den unautorisierten Zugriff auf das SCADA-System; Dallas dokumentierte die Fehlaktivierung der Sirenen durch eine externe Intrusion.

Das zweite Muster betrifft die begrenzte Wirksamkeit rein klassischer IT-Sicherheitslogiken in OT-Kontexten. Zwar spielen bekannte Sicherheitsprinzipien wie Authentifizierung, Zugangskontrolle und Netztrennung in allen Fällen eine Rolle, jedoch zeigt sich jeweils ein prozess- und architekturspezifischer Kontext. Im Ukraine-Fall war die operationale Wirkung erst durch den Missbrauch echter Steuerfunktionen auf der OT-Ebene möglich; in Oldsmar wurde ein prozesskritischer Parameter manipuliert; in Dallas führte eine Schwäche im Signalpfad unmittelbar zur physischen Auslösung des Warnsystems [7, 8, 11]. Daraus folgt, dass OT-Security nicht allein als Erweiterung der IT-Sicherheit verstanden werden kann, sondern eine funktionale Betrachtung physischer Prozesse, Kommunikationspfade und betrieblicher Randbedingungen erfordert [3, 4].

Das dritte Muster betrifft organisatorische und strukturelle Einflussfaktoren. In allen drei Fällen war die Angriffswirksamkeit nicht nur technisch bedingt, sondern auch durch begrenzte Sicherheitsgovernance, unzureichende Vorbereitung auf Störfälle oder fehlende bzw. nicht ausreichend wirksame Überwachungs- und Reaktionsprozesse verstärkt [6,10,12]. Besonders deutlich wird dies im Oldsmar-Fall, in dem die unmittelbare Schadensverhinderung maßgeblich auf der Aufmerksamkeit eines Bedieners beruhte, sowie im Dallas-Fall, in dem der Angriff Folgewirkungen auf Notruf- und Krisenkommunikationsstrukturen hatte [41,42]. Diese Befunde stützen die Annahme, dass OT-Security in kritischen Smart-City-Infrastrukturen wesentlich von der organisatorischen Reife der Betreiber abhängt und nicht allein durch technische Schutzmaßnahmen zu gewährleisten ist. CISA/FBI/EPA betonten nach Oldsmar die Bedeutung

von Zugangskontrollen und Wassersektor-Sicherheitsmaßnahmen; Dallas adressierte nach dem Vorfall direkte Sicherheitsnachrüstungen am Sirenensystem.

5.2 Erklärungsmuster und Mechanismen

Über das bloße Identifizieren gemeinsamer Muster hinaus zielt die Cross-Case-Analyse darauf ab, zugrunde liegende Erklärungsmuster sichtbar zu machen. Die drei Fälle legen nahe, dass der Angriffserfolg jeweils auf einem gemeinsamen Mechanismus beruhte: Ein digitaler oder funkbasierter Zugangspfad ermöglichte die Einwirkung auf einen physischen Prozess, wobei technische Schutzdefizite und organisatorische Schwächen zugleich vorlagen. Der Mechanismus lässt sich damit als Kopplung von Zugänglichkeit, unzureichender Kontrolle und physischer Prozesswirksamkeit beschreiben [7, 18, 19].

Im Ukraine-Fall manifestiert sich dieser Mechanismus in der Kopplung von IT-Kompromittierung, mangelnder OT-Abgrenzung und dem Missbrauch legitimer Steuerfunktionen. Der Angriff

war hochkomplex, aber sein Erfolg beruhte letztlich darauf, dass digitale Zugriffe bis in prozessrelevante Umgebungen hinein möglich waren und dort nicht wirksam begrenzt wurden [39,40]. Im Oldsmar-Fall war derselbe Grundmechanismus in einer deutlich einfacheren Form erkennbar: Ein Fernzugriff eröffnete unmittelbaren Zugriff auf eine prozessnahe Bedienoberfläche, wodurch die Manipulation chemischer Parameter prinzipiell möglich wurde [41]. Im Dallas-Fall wiederum war der Zugangspfad nicht netzbasiert, sondern funktechnisch; dennoch blieb der Mechanismus vergleichbar, weil ein unzureichend geschützter Kommunikationskanal direkt eine physische Wirkung im urbanen Raum auslöste [42].

Daraus lässt sich ein zweites Erklärungsmuster ableiten: Je näher ein Kommunikations- oder Fernzugangspfad an einem physischen Prozess liegt, desto geringer ist die Fehlertoleranz des Systems und desto höher ist die sicherheitsrelevante Wirkung einer Kompromittierung. Dieses Muster erklärt, warum bereits relativ einfache Angriffsformen – etwa ein unzureichend kontrollierter Remote Access oder ein nachahmbares Funksignal – erhebliche Folgen haben können, obwohl sie technisch weniger komplex erscheinen als mehrstufige APT-artige Angriffe [3, 11].

Ein drittes Erklärungsmuster betrifft die Rolle organisatorischer Resilienz. Die Fälle zeigen, dass technische Defizite dann besonders folgenreich werden, wenn Organisationen nicht über klare Sicherheitsverantwortlichkeiten, angemessene Überwachungsmechanismen und belastbare Notfallprozesse verfügen [6,12]. Daraus folgt analytisch, dass die Verwundbarkeit kritischer Smart-City-Infrastrukturen nicht nur eine Funktion ihrer Technologie, sondern auch ihrer institutionellen und betrieblichen Einbettung ist. Genau hierin liegt ein zentraler Beitrag der vorliegenden Arbeit: Die Einzelfälle zeigen unterschiedliche Angriffsformen, die Cross-Case-Analyse macht jedoch sichtbar, dass ihnen gemeinsame soziotechnische Mechanismen zugrunde liegen.

5.3 Verdichtete fallübergreifende Befunde

Die nachfolgenden Befunde stellen die zentrale analytische Verdichtung der vorliegenden Arbeit dar. Während die Rekonstruktion der einzelnen Vorfälle auf dokumentierten Primär- und Sekundärquellen basiert, ergeben sich die folgenden Erkenntnisse aus der vergleichenden Auswertung der drei Fallstudien im Rahmen der Cross-Case-Analyse. Es handelt sich somit nicht um eine bloße Zusammenfassung der Literatur, sondern um eigenständig erarbeitete fallübergreifende Befunde, die auf dem systematischen Vergleich der untersuchten Sicherheitsvorfälle beruhen.

Erstens: Übergänge, Schnittstellen und Zugangspfade bilden die zentrale Verwundbarkeitszone kritischer Smart-City-Infrastrukturen. Die Cross-Case-Analyse zeigt, dass in allen drei Fällen der Angriffserfolg maßgeblich an einem spezifischen Zugangspfad ansetzte. Im Ukraine-Fall war dies der Übergang von der Office-IT in die OT-Umgebung, im Oldsmar-Fall ein bestehender Fernzugriff auf ein prozessnahes System und im Dallas-Fall ein unzureichend abgesicherter funkbasierter Steuerkanal. Die eigene fallübergreifende Analyse legt damit nahe, dass die sicherheitskritischsten Schwachstellen nicht primär innerhalb einzelner Komponenten liegen, sondern an den Übergängen zwischen Systemebenen, Kommunikationswegen und Steuerungsschnittstellen. Diese Befundlage verdichtet die Einzelfälle zu dem übergeordneten Muster, dass Konnektivität und Erreichbarkeit die wesentlichen Einfallstore physisch wirksamer Cyberangriffe darstellen.

Zweitens: Der Angriffserfolg beruht nicht auf isolierten Einzelschwachstellen, sondern auf dem Zusammenwirken technischer und organisatorischer Defizite. Der Vergleich der drei Fälle zeigt, dass technische Schwächen allein den Vorfallverlauf nicht hinreichend erklären. Vielmehr wurde in allen Fällen deutlich, dass unzureichende Authentifizierung, fehlende Segmentierung oder unsichere Kommunikationswege mit organisatorischen Faktoren wie unklaren Zuständigkeiten, begrenzter Sicherheitsüberwachung, schwachem Zugriffsmanagement oder unzureichender Krisenvorbereitung zusammenwirkten. Die eigene Cross-Case-Analyse führt damit zu dem Befund, dass OT-Sicherheitsvorfälle in kritischen Smart-City-Infrastrukturen als soziotechnische Störungsereignisse verstanden werden müssen. Die Verwundbarkeit entsteht nicht nur aus technischen Eigenschaften der Systeme, sondern ebenso aus ihrer organisatorischen Einbettung und der institutionellen Reife der Betreiberstrukturen.

Drittens: Frühzeitig erkennbare Angriffsvektoren liegen vor allem dort vor, wo atypische Zugriffe, unplausible Prozessänderungen oder ungewöhnliche Steuerbefehle systematisch detektiert werden können. Die fallübergreifende Analyse zeigt, dass sich in allen drei Fällen prinzipiell Ansatzpunkte für eine frühere Erkennung identifizieren lassen. Im Ukraine-Fall wären ungewöhnliche Bewegungen zwischen IT- und OT-Bereichen, im Oldsmar-Fall untypische Eingriffe in chemische Dosierungsparameter und im Dallas-Fall nicht plausible Aktivierungssignale des Warnsystems potenzielle Indikatoren für eine Anomalie gewesen. Daraus ergibt sich als eigener analytischer Befund, dass frühzeitige Erkennbarkeit weniger von der absoluten Komplexität eines Angriffs abhängt, sondern vielmehr davon, ob Betreiber in der Lage sind, sicherheitsrelevante

Abweichungen entlang prozesskritischer Kommunikations- und Steuerungspfade systematisch zu überwachen. Genau an dieser Stelle setzt die Ableitung belastbarer Handlungsfelder für Betreiber und Kommunen an.

Zusammenfassend zeigt die Cross-Case-Analyse, dass die drei untersuchten Vorfälle trotz ihrer sektoralen und technischen Unterschiede auf gemeinsame Grundmuster verweisen. Die Eigenleistung der vorliegenden Arbeit besteht darin, diese Gemeinsamkeiten nicht nur fallspezifisch zu beschreiben, sondern sie systematisch zu verdichten und als fallübergreifende Befunde für die OT-Security in kritischen Smart-City-Infrastrukturen herauszuarbeiten.

6. Handlungsfelder, theoretische Einordnung und Fazit

Die vorliegende Arbeit zielt nicht auf die Entwicklung konkreter technischer Einzelmaßnahmen, sondern auf die Ableitung übertragbarer Handlungsfelder und theoretisch verdichteter Zusammenhangsaussagen aus der vergleichenden Analyse dokumentierter Sicherheitsvorfälle. Die wissenschaftliche Leistung besteht somit darin, aus den Einzelfällen generalisierbare Muster typischer Verwundbarkeitskonstellationen in kritischen Smart-City-Infrastrukturen herauszuarbeiten [18–20].

Grundlage der folgenden Ausführungen sind die im Rahmen der Cross-Case-Analyse identifizierten fallübergreifenden Befunde: die besondere Verwundbarkeit von Schnittstellen und Zugangspfaden, das Zusammenwirken technischer und organisatorischer Defizite sowie die Relevanz prozessnaher Anomalieerkennung.

Die nachfolgenden Handlungsfelder ergeben sich aus der vergleichenden Verdichtung der drei analysierten Fälle. Während Literatur und Fallquellen der Rekonstruktion und Einordnung dienten, stellt ihre systematische Bündelung zu übertragbaren Handlungsfeldern die Eigenleistung der vorliegenden Arbeit dar [18, 19].

Die Analyse zeigt, dass in allen drei Fällen ein spezifischer Zugangspfad den Angriff ermöglichte: der IT-/OT-Übergang im Ukraine-Fall, der Fernzugriff im Oldsmar-Fall und der funktechnische Steuerkanal im Dallas-Fall. Daraus folgt, dass Sicherheitsarchitekturen nicht primär komponenten-, sondern schnittstellenzentriert gestaltet werden müssen. Besonders schutzbedürftig sind daher Fernzugriffe, Wartungsschnittstellen, Leitstellenzugänge und drahtlose Kommunikationskanäle. Technisch verweist dies auf Segmentierung, Zonenbildung, Authentifizierung und restriktive Zugriffskontrollen [3, 8, 25, 27].

Ein weiterer zentraler Befund ist, dass der Angriffserfolg nicht allein auf technische Schwächen zurückzuführen war. Vielmehr wirkten in allen Fällen organisatorische Defizite wie unklare Zuständigkeiten, schwaches Zugriffsmanagement oder unzureichende Krisenvorbereitung mit technischen Verwundbarkeiten zusammen. OT-Security ist daher als soziotechnische Steuerungsaufgabe zu verstehen. Zu den wesentlichen Handlungsfeldern zählen die klare Koordination von IT- und OT-Verantwortlichkeiten, die Formalisierung privilegierter Zugriffe sowie belastbare Incident-Response- und Governance-Strukturen [6, 10, 12].

Die Cross-Case-Analyse zeigt zudem, dass in allen drei Fällen prinzipiell früh erkennbare Anomalien vorhanden waren, etwa ungewöhnliche Bewegungen zwischen IT- und OT-Bereichen, untypische Änderungen an Prozessparametern oder unplausible Aktivierungssignale. Daraus folgt die Notwendigkeit eines OT-spezifischen Monitorings, das nicht nur Netzwerkereignisse, sondern auch Steuerbefehle, Prozesswertänderungen und ungewöhnliche Betriebszustände erfasst [7, 11, 25].

Schließlich verdeutlichen alle drei Fälle, dass die Schadenswirkung wesentlich von der Qualität der Reaktion abhängt. Manuelle Wiederherstellung, unmittelbare Intervention des Bedienpersonals oder die schnelle Unterbrechung eines kompromittierten Systems spielten jeweils eine zentrale Rolle. Daraus folgt, dass OT-Security nicht nur präventiv, sondern auch resilienzorientiert gedacht werden muss. Erforderlich sind klare Eskalationswege, vorbereitete alternative Betriebsmodi und belastbare Kommunikationsprozesse [3, 6, 12].

Insgesamt zeigen die abgeleiteten Handlungsfelder, dass OT-Security in kritischen Smart-City-Infrastrukturen nur als mehrschichtiges Zusammenspiel von Schnittstellensicherung, organisatorischer Einbettung, Monitoring und Resilienz wirksam gestaltet werden kann.

Auf Grundlage der fallübergreifenden Befunde lassen sich mehrere Propositionen im Sinne einer theoriegenerierenden Fallstudienanalyse formulieren. Diese dienen nicht der statistischen Verallgemeinerung, sondern der theoretischen Verdichtung typischer Wirkzusammenhänge [18–20].

Proposition 1: Je stärker OT-Systeme kritischer Smart-City-Infrastrukturen über externe, systemübergreifende oder drahtlose Zugangspfade erreichbar sind, desto höher ist ihre Verwundbarkeit gegenüber physisch wirksamen Cyberangriffen.

Proposition 2: Der Erfolg von OT-Sicherheitsangriffen in kritischen Smart-City-Infrastrukturen wird wesentlich durch das Zusammenwirken technischer Schwachstellen und organisatorischer Defizite begünstigt.

Proposition 3: Je näher ein kompromittierbarer Kommunikations- oder Steuerungspfad an einem physischen Prozess liegt, desto höher ist das potenzielle Schadensausmaß bereits bei vergleichsweise einfachen Angriffsformen.

Proposition 4: Die frühzeitige Erkennung von OT-Angriffen hängt maßgeblich davon ab, ob ungewöhnliche Zugriffe, atypische Steuerbefehle und unplausible Prozessänderungen entlang prozesskritischer Pfade systematisch überwacht werden.

Proposition 5: Die Resilienz kritischer Smart-City-Infrastrukturen wird nicht nur durch Präventionsmaßnahmen bestimmt, sondern ebenso durch die Fähigkeit, im Störfall kontrolliert in sichere oder alternative Betriebsmodi überzugehen.

6.1 Einbettung in die Literatur

Die im Rahmen der Fallstudien und der Cross-Case-Analyse gewonnenen Ergebnisse lassen sich sowohl in die OT-/ICS-Security-Literatur als auch in die Forschung zu Smart Cities und kritischen

Infrastrukturen einordnen. Ziel dieses Kapitels ist es, die eigenen Befunde mit bestehenden wissenschaftlichen und normativen Ansätzen abzugleichen und ihren spezifischen Beitrag herauszuarbeiten.

Die OT-/ICS-Security-Literatur betont, dass industrielle Steuerungs- und Leitsysteme besonderen Sicherheitslogiken unterliegen, die sich nicht ohne Weiteres aus klassischen IT-Sicherheitsansätzen ableiten lassen [3,4,11,25]. Insbesondere hohe Verfügbarkeitsanforderungen, lange Lebenszyklen, proprietäre Protokolle und eingeschränkte Patchmöglichkeiten prägen die Sicherheitslage von OT-Umgebungen [3, 7]. Die Ergebnisse der vorliegenden Arbeit bestätigen diese Grundannahme deutlich.

Ein zentrales Ergebnis der Cross-Case-Analyse ist, dass Übergänge, Schnittstellen und Zugangspfade die wesentliche Verwundbarkeitszone darstellen. Dieser Befund steht im Einklang mit den in der OT-/ICS-Security-Literatur etablierten Prinzipien der Segmentierung, Zonenbildung und kontrollierten Kommunikationsbeziehungen [8, 27]. Die vorliegende Arbeit erweitert diese Perspektive jedoch insofern, als sie zeigt, dass sicherheitskritische Schnittstellen nicht nur klassische IT-/OT-Übergänge umfassen, sondern auch Fernzugriffe und funkbasierte Steuerungskanäle.

Auch der zweite Befund, nämlich das Zusammenwirken technischer und organisatorischer Defizite, stimmt mit der bestehenden Literatur überein. Leitfäden und Standards betonen, dass technische Schutzmaßnahmen nur dann wirksam sind, wenn sie durch geeignete organisatorische Prozesse, Rollenmodelle und Sicherheitsroutinen ergänzt werden [3, 12, 25]. Die vorliegende Arbeit bestätigt diese Sichtweise anhand realer Vorfälle und zeigt, dass erfolgreiche Angriffe regelmäßig auf einer Kombination technischer Exponiertheit und organisatorischer Schwächen beruhen.

Darüber hinaus stützen die Ergebnisse die in der OT-Sicherheitsliteratur hervorgehobene Bedeutung prozessnaher Detektions- und Monitoringfähigkeiten. In allen drei Fällen ließen sich potenzielle Anzeichen identifizieren, die auf ungewöhnliche Steuerbefehle, unplausible Prozessänderungen oder atypische Kommunikationsmuster hinweisen [7, 11, 25]. Damit bestätigt die Arbeit die bestehende Literatur, überträgt diese Erkenntnisse jedoch

sektorübergreifend auf unterschiedliche Smart-City-Infrastrukturen.

Die Smart-City-Literatur beschreibt urbane Räume vor allem als digital vernetzte, datengetriebene und sektorübergreifend integrierte Systeme [1, 2, 5]. Demgegenüber betont die Literatur zu kritischen Infrastrukturen die besondere gesellschaftliche Relevanz jener Systeme, deren Ausfall erhebliche Folgen für Versorgungssicherheit und öffentliche Ordnung haben kann [6]. Die Ergebnisse der vorliegenden Arbeit verbinden beide Perspektiven, indem sie zeigen, dass die Digitalisierung urbaner Infrastrukturen neue verwundbare Konnektivitätsstrukturen schafft, die in kritischen Bereichen unmittelbare physische und gesellschaftliche Auswirkungen entfalten können.

Ein wesentlicher Beitrag der Arbeit liegt darin, den häufig eher abstrakten Smart-City-Diskurs um eine konkrete sicherheitsbezogene Fallperspektive zu ergänzen. Während Smart-City-Literatur häufig auf Innovationspotenziale und Effizienzgewinne fokussiert [1, 2], zeigt die vorliegende Analyse anhand realer Sicherheitsvorfälle, dass urbane Digitalisierung gerade dann sicherheitskritisch wird, wenn sie mit OT-Systemen und physischen Prozessen verknüpft ist.

Zugleich bestätigt die Arbeit zentrale Annahmen der CI-Literatur, wonach Verwundbarkeit nicht allein durch technische Schwächen entsteht, sondern durch das Zusammenwirken technischer, organisatorischer und institutioneller Faktoren [6]. Die Cross-Case-Analyse zeigt darüber hinaus, dass eine sektorübergreifende Betrachtung im Smart-City-Kontext besonders erkenntnisreich ist, weil sich trotz infrastrukturspezifischer Unterschiede gemeinsame Verwundbarkeitsmuster identifizieren lassen.

Zusammenfassend bestätigt die vorliegende Arbeit zentrale Annahmen der OT-/ICS-Security-, Smart-City- und CI-Literatur, insbesondere hinsichtlich der Relevanz von Schnittstellen, soziotechnischen Verwundbarkeiten und Resilienzanforderungen. Ihr eigenständiger Beitrag liegt jedoch in der vergleichenden Analyse realer OT-Sicherheitsvorfälle aus unterschiedlichen kritischen Smart-City-Infrastrukturen und der daraus abgeleiteten sektorübergreifenden Verdichtung gemeinsamer Muster und Handlungsfelder.

6.2 Zusammenfassung, Limitationen und Ausblick

Ziel der vorliegenden Arbeit war es, durch eine vergleichende Analyse ausgewählter OT-Sicherheitsvorfälle in Smart Grids, Wasser- und Abwassersystemen sowie intelligenten Verkehrsleitsystemen wiederkehrende Angriffsvektoren, strukturelle Schwachstellen und daraus ableitbare Handlungsfelder zu identifizieren. Zur Beantwortung der Forschungsfrage wurden der Angriff auf das ukrainische Stromnetz (2015), der Vorfall im Wasserwerk Oldsmar (2021) sowie der Angriff auf das Sirenensystem der Stadt Dallas (2017) untersucht und im Rahmen einer Cross-Case-Analyse vergleichend ausgewertet.

Die Ergebnisse zeigen, dass sich tatsächlich wiederkehrende Muster über die drei Fälle hinweg identifizieren lassen. Besonders deutlich wurde, dass Übergänge, Schnittstellen und Zugangspfade die zentrale Verwundbarkeitszone kritischer Smart-City-Infrastrukturen darstellen. Darüber hinaus wurde sichtbar, dass erfolgreiche Angriffe nicht allein auf technischen Schwachstellen beruhen, sondern regelmäßig durch das Zusammenwirken technischer und organisatorischer Defizite begünstigt werden. Schließlich zeigte die Analyse, dass frühzeitig erkennbare Angriffsvektoren prinzipiell vorhanden sind, sofern atypische Zugriffe, ungewöhnliche Steuerbefehle oder unplausible Prozessänderungen systematisch überwacht werden.

Aus diesen Befunden konnten mehrere generalisierbare Handlungsfelder abgeleitet werden. Dazu zählen insbesondere die Absicherung von Schnittstellen und Zugangspfaden, die stärkere Integration technischer und organisatorischer Sicherheitsmechanismen, der Aufbau prozessnaher Monitoring- und Detektionsfähigkeiten sowie eine resilienzorientierte Notfall- und Wiederanlaufplanung. Die Forschungsfrage kann damit dahingehend beantwortet werden, dass

eine vergleichende Analyse realer OT-Sicherheitsvorfälle geeignet ist, wiederkehrende Angriffsvektoren und strukturelle Schwachstellen sichtbar zu machen und daraus übertragbare Handlungsfelder für die Absicherung kritischer Smart-City-Infrastrukturen abzuleiten.

Die Aussagekraft der vorliegenden Arbeit ist durch mehrere Limitationen begrenzt. Erstens basiert die Analyse auf einer kleinen Zahl von drei Fällen, sodass die Ergebnisse theoriegenerierenden, nicht jedoch statistisch repräsentativen Charakter besitzen. Zweitens stützt sich die Arbeit auf sekundäre Datenquellen, deren Vollständigkeit von der veröffentlichten Dokumentation der jeweiligen Vorfälle abhängt. Drittens erschwert die Heterogenität der betrachteten Infrastrukturen eine vollständige Vergleichbarkeit der Fälle, auch wenn gerade diese Vielfalt für die fallübergreifende Analyse erkenntnisreich war. Schließlich werden in der Arbeit keine konkreten Maßnahmen empirisch auf ihre Wirksamkeit hin evaluiert; die abgeleiteten Handlungsfelder bleiben daher auf einer konzeptionellen Ebene.

Für zukünftige Forschung bietet es sich an, die Fallbasis auf weitere Smart-City-Infrastrukturen auszudehnen und die hier entwickelten Befunde durch zusätzliche Fallstudien, Experten-interviews oder quantitative Untersuchungen weiter zu überprüfen. Ebenso wäre eine stärkere Verknüpfung mit etablierten Reifegrad- oder Sicherheitsframeworks sinnvoll, um die praktische Anwendbarkeit der Ergebnisse weiter zu konkretisieren.

Für die Praxis verdeutlicht die Arbeit, dass OT-Security in Smart Cities nicht als isolierte technische Spezialfrage verstanden werden darf. Vielmehr ist ein integrierter Sicherheitsansatz erforderlich, der technische Härtung, organisatorische Governance, prozessnahes Monitoring und resilienzorientierte Notfallplanung zusammenführt. Die zunehmende Digitalisierung urbaner Infrastrukturen wird die Relevanz dieser Fragestellungen weiter erhöhen. Damit unterstreicht die vorliegende Arbeit die Notwendigkeit, reale Sicherheitsvorfälle nicht nur als Einzelfälle zu betrachten, sondern als empirische Grundlage für eine systematische Weiterentwicklung der Sicherheitsarchitekturen kritischer Smart-City-Infrastrukturen.

Literatur

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi. “Internet of Things for Smart Cities.” IEEE Internet of Things Journal, Vol. 1, No. 1, 2014, pp. 22–32.

[2] S. E. Bibri. Smart Sustainable Cities of the Future. Springer, 2018.

[3] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn. Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev. 2. National Institute of Standards and Technology, 2015.

[4] E. Knapp, J. Langill. Industrial Network Security. Syngress, 2014.

[5] C. Harrison et al. “Foundations for Smarter Cities.” IBM Journal of Research and Development, Vol. 54, No. 4, 2010.

[6] S. Bauer, M. Bötticher. Critical Infrastructure Protection. Springer, 2017.

[7] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

[8] International Electrotechnical Commission (IEC). IEC 62443 – Industrial communication networks – Network and system security. IEC Standard Series.

[9] M. H. Cintuglu, O. A. Mohammed, K. Akkaya. “A Survey on Smart Grid Cyber-Physical System Testbeds.” IEEE Communications Surveys & Tutorials, 2017.

[10] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Cities. ENISA Report, 2019.

[11] R. Krutz. Industrial Control Systems Security. Wiley, 2016.

[12] International Organization for Standardization (ISO). ISO/IEC 27001: Information Security Management Systems. ISO Standard.

[13] European Union. Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive). Official Journal of the European Union, 2016.

[14] N. Döring. Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften. 6., vollständig überarbeitete und erweiterte Auflage. Springer, 2023.

[15] P. Mayring. Qualitative Inhaltsanalyse: Grundlagen und Techniken. 12. Auflage, Beltz, 2015.

[16] M. Q. Patton. Qualitative Research & Evaluation Methods. 4th ed., Sage, 2015.

[17] C. Helfferich. Die Qualität qualitativer Daten. 5. Auflage, Springer VS, 2019.

[18] R. K. Yin. Case Study Research and Applications: Design and Methods. 6th ed., Sage, 2018.

[19] K. M. Eisenhardt. Building Theories from Case Study Research. Academy of Management Review, 14(4), 532–550, 1989.

[20] K. M. Eisenhardt and M. E. Graebner. Theory Building from Cases: Opportunities and Challenges. Academy of Management Journal, 50(1), 25–32, 2007.

[21] U. Kuckartz. Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung. Beltz Juventa, 2018.

[22] G. A. Bowen. Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2), 27–40, 2009.

[23] U. Flick. Qualitative Sozialforschung: Eine Einführung. Rowohlt, 2014.

[24] S. Lamnek. Qualitative Sozialforschung. 5. Auflage, Beltz, 2010.

[25] National Institute of Standards and Technology (NIST). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Revision 2, 2015.

[26] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Grids. ENISA Report, 2019.

[27] International Electrotechnical Commission (IEC). IEC 62443 Series: Industrial communication networks – IT security for networks and systems. Parts 1-1, 2-1, 3-3, 4-1.

[28] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber-Attack Against Ukrainian Critical Infrastructure. Alert (IR-ALERT-H-16-056-01), U.S. Department of Homeland Security, 2016.

[29] E-ISAC and SANS ICS. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems, 2016.

[30] U.S. Department of Homeland Security. Assessment of Electricity Disruption Incident Response Capabilities. 2017.

[31] Pinellas County Sheriff’s Office. Press Conference on Oldsmar Water Treatment Facility Cyber Intrusion. Pinellas County, Florida, 2021.

[32] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Environmental Protection Agency (EPA). Compromise of U.S. Water Treatment Facility. Joint Cybersecurity Advisory, 2021.

[33] Cybersecurity and Infrastructure Security Agency (CISA). Top Cyber Actions for Securing Water Systems. CISA Guidance, 2021.

[34] City of Dallas. Emergency Supplemental Addendum. Dallas City Council Meeting Documents, April 12, 2017.

[35] City of Dallas Office of Emergency Management. Outdoor Warning System. City of Dallas, 2017.

[36] Associated Press. “Lack of encryption blamed for false Dallas emergency sirens.” Associated Press, April 11, 2017.

[37] A. Greenberg. “That Dallas Siren Hack Wasn’t Novel—It Was Just Really Loud.” Wired, April 10, 2017.

[38] A. Greenberg. “This Radio Hacker Could Hijack Citywide Emergency Sirens to Play Any Sound.” Wired, August 1, 2018.

[39] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Cyber-Attack Against Ukrainian Critical Infrastructure. IR-ALERT-H-16-056-01, U.S. Department of Homeland Security, 2016.

[40] M. Assante, R. M. Lee, T. Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E-ISAC) and SANS ICS, 2016.

[41] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Environmental Protection Agency (EPA). Compromise of U.S. Water Treatment Facility. Joint Cybersecurity Advisory AA21-042A, 2021.

[42] City of Dallas. Emergency Supplemental Addendum. Dallas City Council Meeting Documents, April 12, 2017.