TRANSKRYPCJA – Odcinek XIII

Bezpieczeństwo krytyczne pod lupą

[00:00:06]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. Do tej pory w naszym cyklu skupialiśmy się głównie na temat ochrony infrastruktury IT, użytkowników i systemów IT. A co z resztą? Nadrabiamy to dzisiaj. Infrastruktura krytyczna pod lupą, bezpieczeństwo ICT/OT. Wraz z moim dzisiejszym gościem przyjrzymy się, na co jest narażona tego typu infrastruktura i jak mogą ją wykorzystać napastnicy, a także jak najlepiej ją zabezpieczać. Moim dzisiejszym gościem jest Wojciech Kubiak – ICT Security Director w PKP Energetyka SA. Posiada praktyczne doświadczenie w obszarach zarządzania bezpieczeństwem IT/OT, audytów bezpieczeństwa IT/OT, bezpieczeństwa infrastruktury krytycznej, bezpieczeństwa fizycznego i środowiskowego, zapobieganie inwigilacji technicznej rozwoju i zarządzania architekturą bezpieczeństwa korporacyjnego. Posiadacz wielu bardzo cenionych certyfikatów ze środowiska cyberbezpieczeństwa, absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej, członek ISSA Polska, autor publikacji dotyczących bezpieczeństwa systemów automatyki przemysłowej i doświadczony trener z zakresu bezpieczeństwa IT/OT. Panie Wojciechu, bardzo się cieszę, że jest Pan dzisiaj tutaj z nami.

Wojciech Kubiak: No trudno powiedzieć, że ja się nie cieszę. Dzielenie się wiedzą to dobry pomysł, w związku z powyższym to spotkanie. Także bardzo, bardzo powiedziałbym rzeczowe, czyli tanie. No zakładam, że będziemy gadać o czymś innym, niż o mnie.

Prowadzący: Panie Wojciechu, zanim przejdziemy do treści naszego dzisiejszego tematu, chciałbym Pana zapytać, czym zajmuje się Pana zespół w PKP Energetyka? Jakie są jego codzienne zadania?

Wojciech Kubiak: A, no w zasadzie tak samo jak każdy zespół cybersecurity. To jest dokładnie to samo, czyli robimy nic, trzymamy nogi na biurkach i udajemy, że wszystko się dzieje dobrze.

Prowadzący: Wszystko samo działa.

Wojciech Kubiak: Tak. Tak naprawdę właśnie taki jest cel ćwiczenia. Natomiast nie do końca to wychodzi, bo tak jak wiemy doskonale otoczenie jest superzmienne, więc nie da się trzymać nóg na biurku. No na koniec dnia odpowiadamy za ten krajobraz cyberbezpieczeństwa, zarówno w świecie tym backofficowym, czyli IT, jak i w naszym korpbiznesie, czyli automatyce przemysłowej. Czyli nasze zdalne sterowanie, telemetria tak, są różne obszary automatyki, za które odpowiadamy pod względem właśnie bezpieczeństwa związanego z systemami różnego rodzaju tak, czyli począwszy od tych, gdzie pojawia się system operacyjny, który znamy z dnia codziennego, typu Windows, Linux , skończywszy na takich wbudowańcach, tak to nazwijmy tak, czyli jest jakiś system, który realizuje jakieś zadania. I

teraz bądź mądry i pisz wiersze, i powiedz, że tam jest bezpiecznie. No także wyzwań jest na co dzień dużo.

Prowadzący: Patrząc na Pana doświadczenie, wszędzie przewija się cyberbezpieczeństwo w odniesieniu głównie tak naprawdę do ICS czy IT, głównie ICS. Muszę zadać to pytanie. Skąd u Pana zainteresowanie tym tematem? I jak właśnie Pana ścieżka ewoluowała w kierunku OT?

Wojciech Kubiak: To dość ciekawe pytanie. Tak naprawdę gdzieś na początku swojej kariery, generalnie wywodzę się z energetyki. Skończyłem Technikum Energetyczne i wchodząc w ogóle w obszar związany kiedykolwiek, w jakikolwiek sposób z IT, to był mój drugi wybór. Także zaczynałem, jako osoba, która zna się na procesie wytwórczym, czy to ciepła, czy energii elektrycznej. Bardzo, w bardzo dużych elektrociepłownie znałem od podszewki. To w drugą stronę tak, czyli jak wytwarzamy, w jaki sposób ten proces technologiczny się tworzy, a potem w związku z różnymi nazwijmy to zdarzeniami losowymi udało mi się trafić do IT. Nie miałem wykształcenia w tym obszarze. Ktoś postanowił zainwestować w to, że znam się właśnie na energii elektrycznej, że potrafię zrozumieć, co to znaczy utrzymanie środowiska w serwerowni. Jedna z dużych firm telekomunikacyjnych stwierdziła, że utrzymanie środowiska jest dla nich na tyle ważne, że wolą zainwestować w kogoś, kto nad tym utrzymaniem środowiska potrafi zapanować, a IT się nauczy później. Bo, jakby bądźmy szczerzy tak, zmuszenie inżyniera, informatyka do nauczenia się, co to jest prąd elektryczny czy klimatyzacja, wentylacja, bezprzewodowe zasilanie i tak dalej, i tak dalej, to raczej wyzwanie, któremu nikt nie podoła, bo nie będzie zainteresowany.

[00:05:03]

Wojciech Kubiak: A w drugą stronę, to ma szansę zadziałać? Tak się zdarzyło tak i zacząłem rozwijać swoją wiedzę w obszarze właśnie informatyki. Potem wszedł pomysł, żeby jednak zrobić studia w tym obszarze, bo warto znać od podszewki. A potem pojawił się pomysł na bezpieczeństwo, po tym jak włamałem się do 40 produkcyjnych baz danych. Ktoś wszedł i zapytał – A, może chciałbyś cyber ? Na koniec dnia już nam udało się te dwa światy połączyć, czyli informatyk, automatyk i cyberbezpieczeństwo. I pewnego rodzaju pasja w tym obszarze się pojawiła, ponieważ nikt o tym nic nie wie niemalże, i zaczynaliśmy biegać gdzieś tam w roku 2012.

Prowadzący: Panie Wojciechu, zanim przejdziemy do dalszych elementów może powinniśmy słuchaczom przedstawić, czym tak naprawdę są systemy ICT czy OT?

Wojciech Kubiak: To jest dobry pomysł, bo tak naprawdę gdzieś na koniec dnia pojawia się pytanie – ale o czym my rozmawiamy? To są powiedziałbym te systemy, które są tym bezpośrednim linkiem między światem wirtualnym, a fizycznym. I kiedy rozmawiamy o informatyce, mamy z tyłu głowy taki obraz pewnego rodzaju świata wirtualnego, jakieś bazy danych, systemy operacyjne, jakieś systemy zapewniające komunikację. A OT można powiedzieć, to jest praktycznie to samo, ale jednak zupełnie

coś innego, bo na koniec sterujemy czymś, tak. Czyli to są różnego rodzaju sterowniki, to są różnego rodzaju elementy wykonawcze, jak zawory, pompy, rozłączniki szybkie czy innego rodzaju rozłączniki elektryczne. Takie elementy infrastruktury, które potrafią wysterować otoczenia, tak. Potrafią sprawić, że piec martenowski grzeje. Potrafią sprawić, że na linii produkcyjnej dzieją się rzeczy dokładnie założone, czy w świecie profesjonalnej elektroniki produkujemy prąd, czy produkujemy ciepło. Także można powiedzieć, że to są właśnie te elementy wykonawcze, które łączą ten świat wirtualny ze światem fizycznym

Prowadzący: To teraz może przechodząc dalej, czym charakteryzują się właśnie systemy OT, jeżeli chodzi o ruch sieciowy? Co łączy, a co dzieli te dwa światy, czyli IT – OT w tym zakresie?

Wojciech Kubiak: Patrząc z perspektywy ruchu sieciowego, to tak naprawdę mamy też dwa poziomy, tak. Pierwszy podobny do świata informatyki, mamy protokoły, zrozumiałe przez wszystkich, mamy jakieś , mamy protokół TCP, czyli połączeniowy, mamy protokół UTP, czyli bezpołączeniowy. Różnica na tym poziomie tkwi w tym, w jaki sposób ze sobą urządzenia rozmawiają. Tam pojawiają się różnego rodzaju protokoły przemysłowe, takie jak Modbus, Profibus, czy DNP3. I one są naturalnie kapsulowane czy pakowane w ten protokół znany z IT. I to jest ten powiedziałbym niesprawiający większych kłopotów poziom. Oczywiście w cudzysłowie, bo trzeba jeszcze rozumieć, co tak naprawdę w tym protokole sterowania się pojawia. U nas jest drugi poziom niższej gdzie już mamy takie protokoły szeregowe, biegające gdzieś tam po , po szynach karbasowych , czyli generalnie po jakichś tam kablach elektrycznych. Tam mamy poziom sterowania, który jest realizowany na poziomy sygnału elektrycznego. To są te protokoły przemysłowe, w większości przypadków bardzo trudno się tam wpiąć, włączyć, bo to są obwody elektryczne. One muszą być zrównoważone po to, żeby sygnał elektryczny był na poziomie zrozumiałym dla urządzenia, żeby mogło to urządzenie interpretować adekwatnie te 0 i 1 elektryczne. Więc tam wejść na ten poziom oznacza najczęściej destabilizację układu i konieczność ponownego ułożenia na poziomie elektrycznym wszystkiego, więc bardzo trudno jest tam wchodzić.

Prowadzący: Panie Wojciechu, a to, co mnie też zawsze bardzo interesowało, to priorytety dla IT vs. priorytety OT. Wracając do teorii – poufność, integralność, dostępność, tak? Jak te elementy rozkładają swoją wagę w przypadku tych dwóch skrajnie różnych światów? Jak zrównoważyć wymagania systemów do spraw biznesowych i to ciągłości działania?

Wojciech Kubiak: Tutaj trudno jest rozmawiać w sposób jednoznaczny. W obu obszarach mamy ten trójkąt święty, o którym Pan wspomniał, czyli to CIA, czyli poufność, integralność, dostępność.

[00:10:09]

Wojciech Kubiak: No i w świecie IT, w tym backofficowym, który znamy, no jednak dojrzałość i priorytety mówią o tym, że poufność jest tak naprawdę najważniejsza. W związku z powyższym sposób

podejścia do organizacji, tego, co się dzieje w świecie IT jest nastawiona na to, żeby tę poufność zachować na najwyższym poziomie. Po drugiej stronie, gdzie mamy system automatyki przemysłowej tutaj wchodzi w grę sterowanie najczęściej jakimś procesem produkcyjnym. Nie mówię, że poufność nie jest ważna. Kiedyś naturalnie te systemy były po prostu odseparowane od otoczenia. Natomiast akcent jest położony na dostępność, tak. Dostępność jest królem. To availability rządzi i w związku z powyższym inne rzeczy są troszkę w cieniu.

Prowadzący: Czyli system tak naprawdę musi zawsze działać?

Wojciech Kubiak: Tak. To są systemy, które bardzo często działają kilka lat bez wyłączeń, tak. Nie wiem, w energetyce na przykład najczęściej ten cykl pracy to jest 7 lat, tak. Zespół elektroenergetyczny, czyli jakaś turbina plus otoczenie raz na 7, 8 lat jest odstawiony do remontu, to oznacza, że po prostu te wszystkie systemy, urządzenia działają bezprzerwowo tak, przez ten cały długi czas. Tam nie ma miejsca na tak zwane , tak powinniśmy nazywać w IT, a mam tam przerwę serwisową w piątek wieczorem, więc spokojnie odstawię, spatchuje i tak dalej, i tak dalej. Tutaj nie ma takiej przerwy, ona jest raz na wiele lat.

Prowadzący: Panie Wojciechu, wspomniał Pan również o separacji i teraz też chciałbym jeszcze ruszyć ten temat – separacja IT od OT. W większości opracowań dotyczących cyberbezpieczeństwa separacja jest takim jednym z pierwszych kluczowych elementów, tak. O separacjach mówi się oczywiście bardzo często biorąc pod uwagę IT w celu podziału dostępu na strefy i jednocześnie powiedzmy ograniczenie ekspozycji na ataki. Ale w przypadku sieci OT jest to już po prostu konieczne i wymagane. W jaki bezpieczny sposób można wymieniać informacje pomiędzy produkcją, a systemami biznesowymi w IT?

Wojciech Kubiak: W zasadzie tak sensu stricte, to nie można. Zawsze jest tak, że jak jest ten link fizyczny, to gdzieś na koniec dnia może się pojawić zagrożenie, ale no żądanie biznesu jest proste, tak. Żeby dobrze planować swoje nie wiem, łańcuchy dostaw i inne jakby elementy utrzymania tych procesów biznesowych, to zapotrzebowanie na informacje ze świata produkcyjnego, ze świata OT jest coraz większe, więc niestety te obszary się łączą. Czy da się to zrobić jakoś tam superbezpiecznie? Na koniec dnia jest to gigantyczne wyzwanie. Po prostu dobra praktyka mówi, że powinno się stworzyć swego rodzaju strefy zdemilitaryzowane pmz pomiędzy światami i zapanować nad tym, kto, z kim i w jakim kierunku działa. Bardzo to reglamentować po to, żeby właśnie próbować osiągnąć bezpieczeństwo. Tak mniej więcej jak w świecie IT możemy tę przestrzeń adresową, która ma dostęp do sieci Internetu, którą można od strony Internetu zaadresować czy dotknąć jej tak, wszelkiego rodzaju systemy transakcyjne na przykład w banku wystawione do Internetu. Bardzo podobnie traktujemy ten punkt styku pomiędzy światem automatyki przemysłowej, a światem IT. Nie wspomnę już oczywiście o ekspozycji do Internetu, bo to powiedziałbym, generalnie nie powinno się tak robić, ale są takie sytuacje, kiedy ten dostęp do sieci Internetu jest superkluczowy ze względu na współpracę

na przykład, z jakimiś regulatorami rynku energetycznego, gdzie musimy z otoczenia, ale wtedy też staramy się bardzo, ale to bardzo reglamentować, kto, z kim i dlaczego.

Prowadzący: I tutaj wspomniał Pan też o bardzo ciekawej rzeczy, odnośnie dostępu do Internetu tak, do sieci Internet. Czy izolacja właśnie OT to rzeczywiście brak połączenia z siecią zewnętrzną, bo znane są oczywiście przypadki, że pojedyncze urządzenie wpięte w taką infrastrukturę, która funkcjonowała do tej pory, jako typowy R-GAP mogło doprowadzić do powstania kolejnego styku, a tym samym no wystawić w teorii odseparowaną infrastrukturę na atak?

Wojciech Kubiak: Potencjalnie to powinna być ta pełna separacja, tak.

[00:15:00]

Wojciech Kubiak: Natomiast tam wszędzie, gdzie mamy bardzo duże infrastruktury tak, tak jak na przykład w mojej firmie, gdzie można powiedzieć pokrywamy cały kraj tak, 25 tysięcy kilometrów, torokilometrów, my to tak określamy tak, czyli tej infrastruktury kolejowej, gdzie my musimy dostarczyć energię elektryczną. To jest, no niebagatelny kawałek powiedziałbym, z perspektywy geograficznej. Więc jak Pan się domyśla nasze obiekty elektroenergetyczne są skomunikowane jakby z centralą spółki po to, czy tam z wieloma obiektami w różnych miejscach po to, żeby można było adekwatnie sterować. Realizuje się to oczywiście na poziomie jakiegoś vanu, tak. W wielu przypadkach nie ma możliwości doprowadzenia medium fizycznego, jakim jest światłowód czy ta skrętka przysłowiowa. Więc w grę wchodzą tylko i wyłącznie jakieś obszary operatorskie tak, dostarczane przez firmy telekomunikacyjne Class LT, czy czasem nawet jakiś tam Edge jest czymś wspaniałym tak, jeśli udało się osiągnąć takie prędkości. Więc jest to taki duży układaniec. I jeśli coś się zepsuje, pojawi się jakiś błąd ludzki, może się pojawić ta ekspozycja na Internet. No i to jest element, który na pewno każdy zespół bezpieczeństwa w takich obszarach bardzo pilnuje tak, stara się, żeby tych nazwijmy to przypadkowych linków do sieci Internet nie było.

Prowadzący: Panie Wojciechu, to takie teraz bardzo krótkie pytanie. Przemysłowe systemy bezpieczeństwa – blokujemy czy tylko monitorujemy?

Wojciech Kubiak: I tak, i tak. Tak najprościej mówiąc, tam wszędzie, gdzie mamy pod spodem system operacyjny, bazy danych, takie rozwiązania, które znamy i mamy doświadczenia tak, ze świata IT, każdy atak ukierunkowany przeciwko systemowi operacyjnemu czy jakiemuś innemu elementowi, w mojej ocenie powinniśmy po prostu blokować. Znamy te wektory, nie wpłynie to negatywnie na realizację, że tak powiem zadań. Natomiast, jeśli chodzi o obszar sterowania, czyli już te protokoły, które są odpowiedzialne za utrzymanie w ruchu, w mojej ocenie powinniśmy to tylko i wyłącznie monitorować. Bo mogą się zdarzyć takie sterowania, które zobaczymy raz na rok albo jeszcze rzadziej i jeśli to jest odstawienie bezpieczeństwa, takiego powiedziałbym bezpieczeństwa procesowego, to raczej takie

sterowanie nie jest częste, a gdybyśmy je zablokowali, to moglibyśmy sprowadzić zagrożenie dla życia i zdrowia ludzi, więc na pewno tam blokować niczego nie wolno.

Prowadzący: Panie Wojciechu, a z Pana perspektywy, jakie są takie najbardziej istotne elementy wpływające na poziom bezpieczeństwa systemów OT? Pytanie dosyć rozległe, tak. Natomiast, jeżeli miałby Pan w kilku tak naprawdę punktach podsumować elementy związane właśnie z bezpieczeństwem OT, takie powiedzmy top, to myślę, że byłoby to fajne.

Wojciech Kubiak: To prawda jest taka, żeby coś chronić, to musimy wiedzieć, co chronimy. Więc taką podstawą podstaw jest oczywiście swego rodzaju wiedza na temat środowiska. I to jest chyba największe wyzwanie generalnie tak, bo taka baza CMDB, czyli Configuration Management Database w świecie IT, to jest relatywnie proste, żeby relatywnie oczywiście proste, żeby mieć takie scentralizowane miejsce, w którym wiemy wszystko o komponentach, które wchodzą w skład tej infrastruktury. W świecie automatyki przemysłowej dopóki jest to jeden obiekt, nie wiem, jakaś linia produkcyjna. Tych komponentów jest oczywiście bardzo dużo, ale jakoś tam można pozbierać do kupy tę wiedzę. Natomiast w takich bardzo rozległych infrastrukturach, jak w energetyce, w gazownictwie. Chyba, chyba takim paradygmatem, który jest strasznie trudno osiągnąć, taki króliczek, za którym gonimy, to jest właśnie CMDB dla UTI . No, bo jeśli znamy środowisko, wiemy, czego chronimy, to po pierwsze wiemy, jakie są podatności, po drugie możemy robić to efektywnie. Bo zawsze coś zaczyna od jakiejś niedostępności tak, jakiejś drobnej awarii. Dopiero to się przeradza potem w jakiś incydent, niekoniecznie związany z cybersecurity. Ale jeśli nie mamy tej widoczności, czyli widoczność i wiedza, tak.

[00:20:00]

Wojciech Kubiak: Czyli wiedza, co chronimy i możliwość uzyskania dostępu, też jest w wielu przypadkach bardzo trudna. Więc wydaje mi się, że to są dwa elementy, które sprawią, że możemy mówić, że budujemy bezpieczeństwo dla tego obszaru.

Prowadzący: To chciałbym poruszyć jeszcze kwestię związaną z Mitre Attack. Jakie techniki i narzędzia wykorzystywane są do zakłócenia funkcjonowania systemów przemysłowych? Matryca zawiera w sobie całą tabelę dotyczącą ICT, tak? Jak w praktyce można te informacje wykorzystać w systemach bezpieczeństwa czy procesach związanych z infrastrukturą OT?

Wojciech Kubiak: Znaczy dotąd dopóki dany system automatyki przemysłowej egzystuje na komponentach znanych ze świata IT, to w zasadzie cała, cały ten kij ma zastosowanie, tak. Jeśli w grę wchodzą jakieś specyficzne systemy wbudowane, jak na przykład na sterownikach, gdzie owszem, no jak będą to sterowniki PRC bardzo często niestety mają takie udogodnienia typu Back Server tak, na którym możemy obejrzeć stan urządzenia, stan jakby procesu i tak dalej. Natomiast gdzieś pod spodem oprócz tego drobnego elementu, to już mają taką typową automatykę tak, czyli jakiś program

realizowany na sterowniku. Więc powiedziałbym, patrząc na Mitre – wszystko wchodzi w grę. Tak, wchodzi w grę jakby zebranie informacji o otoczeniu, gdzieś tam dotarcie, zakorzenienie się, okopanie, schowanie, kolejne próby osiągania kolejnych elementów. I tak naprawdę dzisiaj chyba już nie ma takich systemów automatyki przemysłowej, w których nie ma kawałka IT. Więc wszystko może mieć zastosowanie.

Prowadzący: Panie Wojciechu, a analiza i zarządzanie ryzykiem w przypadku systemów przemysłowych. Co należy wziąć pod uwagę? Bo już wspominał Pan, że nieraz problemy już tutaj natury tak naprawdę przemysłowej mogą doprowadzić nawet do, no niebezpieczeństwa tak naprawdę utraty zdrowia i życia różnych ludzi. Więc jak wygląda w tym wypadku tego typu analiza? I czy jest ona też w pewnym sensie podobna do procesów przeprowadzanych w systemach IT?

Wojciech Kubiak: Znaczy podobieństwo zawsze można znaleźć, tak. No analiza ryzyka jest analizą ryzyka. Natomiast jak patrzymy na wpływ na otoczenie i gdzieś na koniec dnia także na obszary regulacyjne, no chociażby z perspektywy Ustawy o krajowym systemie cyberbezpieczeństwa. Kwalifikacja, że mamy incydent powiedziałbym ważny czy poważny oznacza wpływ na otoczenie, tak. Czyli weźmy taki przykład blackoutu czy Ukrainę, kiedy wchodzi w grę odcięcie od prądu elektrycznego nie wiem, kilka milionów odbiorców, to trudno mówić o tym, że nic się nie stało, tak. To nie zawsze jest taki bezpośredni wpływ na życie i zdrowie no, ale wyobraźmy sobie, że w dużej aglomeracji miejskiej nagle ktoś powoduje, że wszystkie światła są zielone. Wygląda to śmiesznie, tak. Natomiast efekt działania oznacza najprawdopodobniej setki, jeśli nie tysiące wypadków drogowych, w których ktoś po prostu może ucierpieć. Więc ta analiza ryzyka musi badać wpływ na otoczenie. To jest kluczowe w tym podejściu, w tym ćwiczeniu. Po prostu musimy się zawsze zastanowić, kto jest odbiorcą, jak to może zaburzyć jakby to życie ludzkie, czy może mieć wpływ na utratę życia bądź zdrowia. Także troszkę bardziej powiedziałbym prawdziwie musimy patrzeć na to, co te systemy sterowania robią. No weźmy pod uwagę budynek. Budynek, który najczęściej dzisiaj jest inteligentnym budynkiem, ma jakiś BMS pod spodem, czyli Building Management System. No i na przykład tak, spowodowanie, że wszystkie systemy dbające o środowisko zamiast latem chłodzić, zaczną grzać. To może być ciekawe z perspektywy pracy biurowej. A na koniec dnia może tak naprawdę zmusić do tego, że wszyscy ludzie muszą przerwać swoją pracę. Więc podstawą to jest patrzenie tak naprawdę, na co te systemy mają wpływ.

Prowadzący: Panie Wojciechu, to prawo i praktyka tak, w przypadku infrastruktury krytycznej. Wspomniał Pan o Ustawie o krajowym systemie cyberbezpieczeństwa. Co znaczy dla tak zwanych operatorów kluczowych, tak? Czym jest Ustawa i co ze sobą niesie dla firm, takich jak PKP Energetyka?

Wojciech Kubiak: Unia Europejska postanowiła wyregulować ten obszar i jakby na podstawie Dyrektywy pojawiły się krajowe implementacje prawne, tak.

[00:25:07]

Wojciech Kubiak: W naszym przypadku jest to Ustawa o krajowym systemie cyberbezpieczeństwa. Ona nakłada na operatorów usług kluczowych szereg wymogów, które w mojej ocenie, to dobrze, że się coś takiego pojawiło, bo jakby nie pozostawia złudzeń, że obszar cyberbezpieczeństwa jest superważny. To dobrze tak, że ktoś się nad tym pochylił. Natomiast z drugiej strony, to niedobrze, bo to oznacza bardzo często dla organizacji spore wydatki, bo trzeba doinwestować ten obszar. A pamiętajmy, że automatyka przemysłowa, czy generalnie systemy produkcyjne to są instalacje, które mają średni czas życia 30+ tak, jeśli chodzi o lata. W przeciwieństwie do świata informatyki, gdzie średni cykl życia rozwiązania to jest około 5 lat. Tutaj mówimy o przedziałach trzydziestoparoletnich. Więc najczęściej firmy infrastrukturalne budowane latami mają ogromny dług technologiczny tak, czyli pojawiają się systemy, które z perspektywy IT dawno już powinny być zrekomercjonalizowane. Tak, więc patrząc jakby z tej perspektywy, Ustawa czy tego rodzaju regulacje są po prostu ogromnym wyzwaniem dla takich firm infrastrukturalnych, dla firm świadczących usługi kluczowe, czy posiadających infrastrukturę krytyczną. Więc ta regulacja jest niezwykle potrzebna. Natomiast też rozciągając to patrzenie dalej, mówiąc o Ustawie o zarządzaniu kryzysowym, gdzie właśnie definiuje się infrastrukturę krytyczną kraju, to tak naprawdę tutaj gdzieś jest taki duży błąd w myśleniu regulatora. Regulator zdaje sobie z tego sprawę w Polsce, więc istnieją jakieś tam inicjatywy, które na koniec dnia wyrównają ten obszar, bo Ustawa o krajowym systemie cyberbezpieczeństwa patrzy na proces, jako całość. Ustawa o zarządzaniu kryzysowym patrzy na obiekty, które są infrastrukturą krytyczną i one mają swój udział w procesie. Natomiast nie zawsze jest tak, że patrzy się na proces tak, patrzy się na konkretny obiekt. Tam, gdzie ta infrastruktura jest typowo osadzona w jednym miejscu ma to uzasadnienie. Natomiast tam wszędzie, gdzie jest to jakaś infrastruktura rozległa, no to proszę mi powiedzieć, w jaki mądry i cudowny sposób z kilku, kilkudziesięciu tysięcy obiektów powiedzieć, że te są krytyczne i te chronimy? Siedem? No bądźmy szczerzy, to jest żart. Gdzieś tu są te nieścisłości i innego rodzaju oczekiwania. Mam nadzieję, że gdzieś na koniec dnia, jakby obie Ustawy się gdzieś spotkają i będzie logiczna relacja pomiędzy tym, jak chronimy obiekt, a jak chronimy proces, jako całość.

Prowadzący: Panie Wojciechu, to drążąc dalej temat, co pomaga, co wręcz przeszkadza we wdrażaniu KSC? Jakie są największe wyzwania? Bo wspomniał Pan o tym, że powoduje to oczywiście zwiększone wydatki, to jest raz. Druga sprawa, to pewne niejasności, które wiążą się również z nieodpowiednimi dokumentami. Ale jeszcze, jeżeli chodzi już tak bezpośrednio o wdrożenie tych elementów, które są opisane między innymi tam w Art.8, gdzie jest mowa o reagowaniu na incydenty bezpieczeństwa, zapobieganiu incydentom bezpieczeństwa, takie dosyć ogólne wyrażenia.

Wojciech Kubiak: Powiem tak, największym problemem jest ta dysproporcja wiedzy pomiędzy właśnie ludźmi z IT, a ludźmi z automatyki przemysłowej, czyli tymi odpowiedzialnymi za ruch. To jest największe wyzwanie. Czyli to wyrównanie wiedzy w obu obszarach i zrozumienie tak, żebyśmy używali tego samego języka. Dla kogoś z IT cybersecurity to jest taki immanentny element tak, tego rozumienia, paradygmatu ciągłości działania. Z perspektywy ludzi odpowiedzialnych za ruch, za automatykę, oni nie rozumieją tego obszaru cyber, nie rozumieją tych elementów związanych właśnie z systemami, sieciami i tak dalej. To jest chyba największe wyzwanie, doprowadzenia do tego, że w tym dialogu obie strony zrozumieją, o czym rozmawiają. Po prostu inne paradygmaty rządzą światami i tak, w momencie, kiedy pojawiają się te obszary wspólne tak, to połączenie światów, no niestety ryzyka się pojawiają. I wydaje mi się, że z perspektywy Ustawy ten timeline tak, ten harmonogram osiągnięcia pewnych elementów, chociażby z perspektywy właśnie reagowania, monitorowania jakby tych zdarzeń w systemach i reagowania na incydenty, nauczenie ludzi, którzy mają oglądać te wszystkie cudowne zegarki i adekwatnie zareagować na incydent, to jest duże wyzwanie.

[00:30:12]

Wojciech Kubiak: Bo tak naprawdę najczęściej ci ludzie nie mają wiedzy. Wiedzą, że jest jakieś zdarzenie, które jest zdarzeniem niepożądanym, ale na 99,9% nie będą wiedzieli, jak adekwatnie zareagować. Czy można to odseparować, jaki to będzie miało wpływ na proces, jako całość. Więc to jest chyba takie clue problemów związanych z implementacją bezpieczeństwa patrząc z perspektywy litery prawa vs. praktyka i utrzymanie ciągłości działania, i bezpieczeństwa jakby tego obszaru.

Prowadzący: Panie Wojciechu, to zostawmy na razie KSC. Co z urządzeniami i systemami automatyki przemysłowej, które nie były projektowane z myślą o cyberbezpieczeństwie w połączenie z obecnym krajobrazem cyberprzestępczości, który dosyć intensywnie się zmienia? Sam Pan wspominał o takiej rzeczywiście długowieczności pewnych elementów, gdzie one muszą pracować przez naprawdę długi czas. W między tak naprawdę czasie pewne elementy się oczywiście mogły pozmieniać. Jak tutaj żyć i jak można dostosować te rozwiązania do obecnej sytuacji?

Wojciech Kubiak: W mojej ocenie jest tylko jedno logiczne podejście, czyli utworzyć standardy dla wszystkich nowych instalacji tak, czyli żeby to, co jest budowane czy przebudowywane, żeby już powstawało, no w takich dobrych praktykach. Czy to , to nie ma znaczenia tam naprawdę, kto te dobre praktyki zebrał w całość. One po prostu są dobre, kropka. Ale zostaje ten ruch technologiczny, o którym wspominałem. Tutaj jest duża trudność, tak. Jak Pan sam zauważył, w tamtych latach nikt nie myślał o tym obszarze cybersecurity. Więc jakby jedynym logicznym podejściem to jest próba stworzenia swego rodzaju bańki, takiej szklaneczki, którą staramy się odseparować od otoczenia. I możemy reagować tak naprawdę incydentalnie tak, czyli musimy być świadomi, że nastąpił incydent, czyli musimy mieć tę widoczność. To jest paradygmat. I musimy mieć dobry backup tak, tej konfiguracji urządzenia. Jeśli ktoś

nam to urządzenie przerobi na cegłę, musimy mieć takie urządzenie zapasowe, gdzieś tam i później mieć możliwość przeprowadzenia tego takiego Forensics, Investigation and Response, tak. Czyli musimy wiedzieć, co się wydarzyło, czyli musimy mieć tę widoczność, musimy mieć logi, musimy mieć możliwość odzyskania backupu, tej dobrej konfiguracji i musimy wiedzieć, jaki był wektor ataku, żeby spróbować to dobezpieczyć, tak. Chyba w większości przypadków tak, jak powiedziałem możemy być reaktywni tylko, więc bez wiedzy o tym, że był incydent. Może dojść do takiej sytuacji, jaka była na przykład w Iranie tak, kiedy doprowadzono do fizycznego uszkodzenia wirówek tych, które miały pomóc w pozyskiwaniu uranu. Czyli ktoś je przesterował tak, te przetworniki częstotliwości, które miały sterować wirówkami, doprowadził do ich fizycznego uszkodzenia. Więc gdzieś bez tej widzialności nie będziemy w stanie dowiedzieć się, jak możemy przeciwdziałać. Chyba to jest jedyne podejście, czyli wiedzieć jak najwięcej, mimo że stoimy obok albo mamy kopię ruchu. Ale kluczowe jest to wejście na ten niższy poziom tak, czyli żeby mieć tę widoczność na poziomie systemów sterowania, w tych protokołach, które nie są tymi protokołami informatycznymi, głębiej tak, na poziomie tych połączeń elektrycznych. Jeśli tam będziemy w stanie coś zobaczyć, to nawet systemy bazujące na sztucznej inteligencji, na tym uczeniu maszynowym będą w stanie powiedzieć, że nie wiem, ten obraz ruchowy, ten obraz sterowania jest dobrym obrazkiem. A w sytuacji, kiedy ktoś fizycznie podejdzie do urządzenia podepnie i zmieni program sterujący, no to statystyka ruchu się zmieni, tak. Czyli to zejście na dół jest superważne, bo w większości przypadków chyba już na poziomie tych protokołów IT będzie za późno.

Prowadzący: Bo pytanie było tak naprawdę nieprzypadkowe, bo w środowisku IT dużo mówi się o patchowaniu, aktualizacji oprogramowania, systemach operacyjnych. A tak, jak sam Pan wspomniał, no pewne elementy sterujące z wbudowanymi czasami systemami, które nie mogą działać z nowymi wersjami albo producent w ogóle na nie przewiduje już aktualizacji, albo producenta już po prostu dawno nie ma. No są to ewidentnie problematyczne, dodatkowo gdzieś to słynne hasło, jak działa to nie ruszaj, prawda?

[00:35:01]

Wojciech Kubiak: To prawda, to jest taki, no paradygmat tak, bezpieczeństwa tak, żeby mówić, że coś jest bezpieczne, no musimy się patchować. To jest takie powiedziałbym, odniosę się do domu, możemy mieć najlepsze zamki w drzwiach, ale w sytuacji, kiedy okno jest otwarte trudno mówić o tym, że jest bezpiecznie. Albo na przykład mamy skrzyneczkę na klucze przed wejściem na posesję tak, i ta skrzyneczka na klucze jest po prostu otwarta. Więc możemy mieć super zamki, natomiast ktoś może wziąć kluczyk i po prostu przekręcić zamek. Nie będzie się bawił w forsowanie drzwi skoro klucz ma dostępny. A podatności, to są takie właśnie klucze wiszące na haczykach, które możemy wziąć i z nich skorzystać. To jest tak, to jest ogromny problem. Ten problem będzie z nami egzystował. Ja ten problem znam z wielu obszarów, bo gdzieś tam na początku, tak jak wspomniałem wywodzę się z

jakiegoś obszaru telekomunikacyjnego i tam mieliśmy podobną walkę z vendorami, tak. Przychodzili ludzie, którzy robili sieci gsmowe, ja im mówiłem – A, co wy tam wiecie o tych systemach, nie znacie się, jest jak jest, tak musicie się przyjąć , koniec. I ten proces uświadamiania vendorów, że skoro jest interfejs IP, to znaczy, że musimy patrzeć także na podatności z tego świata. To jest ta sama walka, która w tej chwili toczy się z vendorami, którzy tworzą systemy do realizacji właśnie procesów produkcyjnych, do tej automatyki. To jest podobny proces, ci vendorzy, którzy pochodzą ze Stanów Zjednoczonych już mają większą świadomość i tam jest dużo łatwiej prowadzić rozmowy, tak. Nadal ci mali vendorzy z rynków lokalnych, no ten proces uświadamiania jest bardzo trudny. No i w większości przypadkach, tak jak Pan wspomniał nie ma, nigdy nie był ten proces patchowania wzięty pod uwagę przy tworzeniu rozwiązania. Jeśli ono bazuje na jakimś systemie operacyjnym, to dzisiaj jasno mówimy dostawcy, tak – musisz w swoim procesie utrzymaniowym wziąć pod uwagę to, że system operacyjny na koniec dnia może być end of life, musimy go wycofać, czyli ty musisz nam dostarczyć możliwość podniesienia wersji tak, nowej tej, która będzie utrzymywana normalnie, musisz nam dać możliwość wgrywania poprawek bezpieczeństwa bezwzględnie, więc ty musisz przeprowadzić testy i dać nam zielone światło, powiedzieć – tak, sprawdziłem u siebie, na ten system na przykład scada nie ma to wpływu tak, możecie patchować ten system i będzie bezpieczny. Więc to jest tak, to jest ogromny problem, ogromne wyzwanie. Ale mówię podstawą podstaw jak zawsze jest możliwość dowiedzenia się, co się dzieje. Niestety powstają jakieś tam odkrywane podatności, także do systemów automatyki, nie tylko tych systemów operacyjnych, które są pod spodem, czy baz danych. Więc, no mówię, dzisiaj vendorzy patchują, wypuszczają nowe firmwary, natomiast ten proces przejścia od systemów, które nie wspierają ten proces do systemów, które będą ten proces wspierały, jest kosztowne czasowo. Musimy po prostu poczekać, aż dany system osiągnie wartość zerową i będzie można go wymienić, będzie to uzasadnione ekonomicznie.

Prowadzące: Wybrano takie te systemy przemysłowe. Wspominał Pan między innymi kwestię elektrowni na Ukrainie, wspominał Pan Iran i Stuxnet. Takich przykładów jest dużo i pojawiają się w miarę regularnie, tak. Mniej lub bardziej wyrafinowane incydenty, które budzą większy bądź mniejszy, jakieś tak naprawdę tutaj skojarzenia z hakerami. Ale jakie są najczęstsze motywacje dla osób przeprowadzających ataki na sieci przemysłowe, z Pana perspektywy?

Wojciech Kubiak: Patrząc tak sensu stricte na motyw wydaje mi się, że na dzień dzisiejszy najczęściej jest to motyw finansowy, bo firmy infrastrukturalne bądź, co bądź posiadają bardzo duże zasoby, tak. Biorąc pod uwagę, no takim majątkiem zarządzają, to muszą dysponować dużymi pieniędzmi. Więc ten motyw finansowy jest bardzo ważny, tak. Prosty przykład Colonial Pipeline w Stanach Zjednoczonych tak, ten dostawca całej infrastruktury ropociągów, czy generalnie rur tak, które połączyły całe

wschodnie wybrzeże Stanów Zjednoczonych i gdzie 45% zapotrzebowania na paliwa płynne, czy to olej napędowy, czy etylinę, czy na koniec dnia także paliwo lotnicze.

[00:40:02]

Wojciech Kubiak: Ta firma dostarczała, pokrywała to zapotrzebowanie. Był atak ransomwarowy, zaszyfrowano infrastrukturę, nie było możliwości prowadzenia ruchu. Pojawiły się oczywiście z automatu ogromne straty finansowe dla takiego przedsiębiorstwa. Więc, nie będę mówił o etyce jakby tego działania, natomiast gdzieś na koniec dnia pojawia się pokusa zapłacenia tego okupu, tak. Jeśli dobrze pamiętam 4,4 mln dolarów firma musiała zapłacić okup. Gdzieś udało się FBI ponad 2 mln dolarów odzyskać, tak powiedziałbym dość przypadkowo, to dobrze. Natomiast ta motywacja finansowa ma znaczenie. I to jest relatywnie prosta sytuacja. Gorzej jest, kiedy w grę wchodzą działania na poziomie rządów. Chociażby właśnie ten Blackout na Ukrainie. No w mojej ocenie to było takie pokazanie siły wręcz z dużym prawdopodobieństwem można powiedzieć, że to jednak Rosjanie pokazali Ukrainie, że mają moc, że są w stanie zrobić różne, brzydkie rzeczy. I to jest ten trudniejszy problem tak, kiedy w grę wchodzą właśnie układy dużych państw, gdzie nie ma problemów jakby ze sfinansowaniem całego procesu, wykryciem tych podatności, zero-day i na koniec dnia przejęcie kontroli, doprowadzenie do sytuacji niepożądanej. Także mi się wydaje, że to są takie dwa najważniejsze aspekty, jeden – siłowy, drugi – finansowy.

Prowadzący: Panie Wojciechu, a czy częściej mamy do czynienia z bezpośrednim atakiem, celowanym na infrastrukturę OT, czy swojego rodzaju rykoszetem odbijanym od infrastruktury IT, która właśnie rozlewa się również na środowiska produkcyjne? Czy w ogóle jest możliwe wykorzystanie takiego scenariusza, jako sieć IT będąca wektorem ataku na sieć OT?

Wojciech Kubiak: Oczywiście to jest najprostszy sposób. Dość często jest tak, że ta automatyka obrywa rykoszetem tak, jeśli nie ma dobrej separacji pomiędzy światem IT, który ma ekspozycję na Internet. Mamy naszych pracowników, oni mają swoje laptopy tak, gdzieś łączą się z domów, z Internetu do infrastruktury, ten , na który przychodzi poczta korporacyjna tak, gdzie, znaczy poczta elektroniczna tam, gdzie możemy oberwać jakimś phishingiem czy tam ręcznym celowanym i zostanie przejęta kontrola nad taką stacją. Tutaj ryzyka są największe i tak jest najczęściej, że ktoś ląduje w świecie IT, rozpycha się i udaje mu się świetnie osiągnąć świat IT. Tak chyba jest najczęściej. Natomiast bywają bardzo duże błędy, powiedziałbym systemowe, kiedy po prostu jest komponent w świecie automatyki przemysłowej, który ma niezamierzoną, bezpośrednią komunikację z siecią Internet. I to jest kłopot. Poprzednio pracowałem w dużych firmach consultingowych, bardzo często robiliśmy audyty takich środowisk automatyki przemysłowej. I bardzo często było tak, że w tej szafie, w której są systemy sterowania odnajdywaliśmy jakiś modem, który zapewniał dostawcy jakiemuś integratorowi dostęp zdalny bez kontroli tak naprawdę danej firmy, która jest właścicielem infrastruktury. I to też jest

niebagatelne ryzyko, bo dość często ci integratorzy po prostu nie myślą o tym aspekcie, tak. I jakby wystawienie jakiegoś modemu, routera, który ma dostęp do sieci Internet i korzysta z jakichś firmwarów, które pozwalają na obejście zabezpieczeń, tak. To jest takie proszenie się po prostu o problemy.

Prowadzący: No właśnie Panie Wojciechu, bezpieczny dostęp zdalny w przypadku sieci OT. Funkcjonuje w ogóle taki ?

Wojciech Kubiak: Funkcjonuje i da się go realizować. Problem polega na tym, że w takich rozległych infrastrukturach zawsze tam szczególnie, gdzie nie ma dobrych, sprawnych łączy, to jest kłopot z wydajnością i zawsze limitujemy tak, co tak naprawdę po tym cienkim drucie w cudzysłowie biega. Ale tak, jest takie podejście. No w mojej ocenie jedyna i słuszna implementacja jest taka, że mamy scentralizowany taki dostęp zdalny. No trudno sobie wyobrazić sytuację, że za policzalne pieniądze ktoś nam będzie świadczył serwis, jeśli będzie musiał fizycznie pojechać na obiekt zawsze. To są niebagatelne kwoty.

[00:45:01]

Wojciech Kubiak: Więc jakby ten dostęp zdalny jest oczekiwany, żeby także, jakby ten proces utrzymania do góry, ekonomicznie do połknięcia. No proszę sobie wyobrazić, że do realizacji zadań takich powiedziałbym serwisowych ktoś, kto wdrożył emersonowy nie wiem, system DCS, jakieś , serwis jest w Stanach i, że ludzie ze Stanów do każdej czynności lecą sobie do Polski. To są bardzo duże pieniądze tak, za taką fizyczną obecność tych ekspertów, którzy są bardzo kosztowni. Bo trzeba im zapłacić tam przelot tak, całą akomodację w Polsce. To oznacza, że w tym czasie nie są w stanie robić innych rzeczy, więc te ceny są bardzo wysokie. Więc ten dostęp bezpieczny serwisowy jest jak najbardziej mile widziany. No i tak jak, jakby do brzegu, powinien być scentralizowany, powinien być jeden punkt dostępu, na jakimś rozwiązaniu klasy PAM, czyli Privileged Acces Management, z zapisem sesji, z taką limitacją tak, że możemy zarządzić tym dostępem zdalnym, żeby on się nie realizował bez naszej kontroli w żaden sposób. Żeby było to zawsze powiązane z jakimś zleceniem pracy, żeby mieć świadomość, kto, kiedy i gdzie, że tak powiem, coś robi, wdraża, ogląda. Żeby mieć właśnie kontrolę pełną nad tym dostępem.

Prowadzący: Moim i Państwa gościem był Wojciech Kubiak – PKP Energetyka. Panie Wojciechu, bardzo dziękuję za Pana obecność.

Wojciech Kubiak: Ja także dziękuję za możliwość podzielenia się odrobiną wiedzy. Mam nadzieję, że informacje, które Państwo usłyszeli odrobinę pomogą w realizacji zadań codziennych w obszarze bezpieczeństwa właśnie automatyki przemysłowej.

Prowadzący: I do następnego odcinka.