TRANSKRYPCJA – Odcinek X

Kilka kroków przed

[00:00:06]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. Moi drodzy, dzisiaj zajmiemy się tematem, nad którym zastanawia się cała masa osób – w jaki sposób możemy być o kilka kroków przed hakerem, przed napastnikiem? Czy jest to w ogóle możliwe? Czy to tylko mrzonka i swojego rodzaju utopia? Przedstawimy troszkę mitów, faktów, ale również statystyk. Kilka kroków przed, czyli jak być lepiej przygotowanym na atak. Moim dzisiejszym gościem jest Paula Januszkiewicz, kobieta renesansu. Paula ma niesamowite doświadczenie w projektach związanych z bezpieczeństwem, założyciel i szef firmy CQURE, poświęca się swoim pasjom jak testy penetracyjne, doradztwo w systemach bezpieczeństwa oraz tworzenie szkoleń i seminariów. Posiadacz tytułu Microsoft NVP, Microsoft Regional Director. Paula, jest mi niezmiernie miło móc Cię dzisiaj z nami gościć.

Paula Januszkiewicz: Absolutnie dzięki wielkie Michał za zaproszenie. Jest mi bardzo, bardzo miło. Tym bardziej, że cyberbezpieczeństwo jest fascynującym tematem i o tym też dzisiaj będziemy rozmawiać.

Prowadzący: Oczywiście, że będziemy rozmawiać. Paula, zanim przejdziemy do tematu chciałbym Cię zapytać, skąd tak naprawdę zamiłowanie do cyberbezpieczeństwa u Ciebie? Jakie były tego początki i co w świecie cybersec sprawia Ci taką największą frajdę?

Paula Januszkiewicz: Wiesz co, generalnie zamiłowanie do cyberbezpieczeństwa w zasadzie można powiedzieć, że mam od samego początku. Dlatego, że to są takie tematy o ogólnie rzecz biorąc, gdzie tak naprawdę po pierwsze się nie nudzisz, a po drugie codziennie pojawia się coś nowego, codziennie jest coś do odkrycia, jak na przykład masz doświadczenia z jakimś klientem i okazuje się, że na przykład dany klient został zhakowany, to bardzo fascynujące jest za każdym razem dochodzenie do tego, co tam tak naprawdę się wydarzyło, przez co każda jedna sytuacja dostarcza ci wrażeń i każda jedna sytuacja jest właśnie taka ekscytująca.

Prowadzący: Czyli po prostu nie nudzisz się w pracy. To też trzeba przyznać

Paula Januszkiewicz: Absolutnie nie. Zwłaszcza w pandemii mamy do czynienia z ogromną ilością projektów związaną z tym, że jakiś klient na przykład właśnie został zhakowany, coś tutaj trzeba podziałać. Więc takich, takich rzeczy dzieje się naprawdę dużo, co zresztą pokazują statystyki. I no cóż, cyberbezpieczeństwo jest bardzo ciekawym, ciekawym, bardzo ciekawą branżą w biznesie, w ogóle w ogólnie pojętym IT i na pewno rozwijającym się, więc coraz więcej osób zaczyna zwracać na to uwagę.

Prowadzący: Wiesz co, mam jeszcze jedno pytanko, bo mocno mnie to ciekawi. Czy możesz coś powiedzieć więcej na temat swojego tytułu NVP, czym jest dla Ciebie, co daje Ci w codziennej pracy? Nie licząc oczywiście no wiadomo, wielkiej satysfakcji, jako ta jedna z wybranych.

Paula Januszkiewicz: Jasne. NVP i też, może w sumie też może trochę powiem o tym Regional Director, bo te rzeczy są ze sobą bardzo powiązane. To jest tytuł, który jest przyznany za osiągnięcia albo generalnie pracę, bym powiedziała, w ramach jakichś community, w ramach jakiejś społeczności. Co też na przykład niekoniecznie oznacza, że trzeba na przykład nie wiem, organizować eventy, być bardzo aktywnym gdzieś tam na jakichś forach. To raczej oznacza, że coś zrobiłeś dla społeczności. Może to być na przykład i udział w jakiejś konferencji, zaangażowanie w jakiejś konferencji, często pro bono, i na przykład no cóż, dostarczyłeś coś, co inni mogą uważać za użyteczne, i tych rzeczy po prostu się gromadzi przez cały rok całkiem sporo. I to jest tytuł, który jest przyznawany za właśnie twoją działalność w poprzednim roku. A Regional Director jest trochę tożsamym tytułem, niemniej jednak bardziej skupiającym się na biznesie. I takich Regional Directors per kraj zwykle jest na przykład jedna bądź też dwie osoby, w zależności od rozmiaru danego kraju. I to są osoby, które są reprezentujące taką poniekąd konwersję innowacji i technologii w coś użytecznego. Czyli na przykład fakt, że istnieje jakaś technologia, no to też o niczym nie świadczy, trzeba ją zrozumieć i w jakiś sposób przedstawić, żeby była po prostu użyteczna dla biznesu. Więc to jest też takie przełożenie trochę technologiczne i trochę biznesowe.

Prowadzący: No Paula, gratulacje.

Paula Januszkiewicz: Dzięki.

Prowadzący: CQURE, Twoja firma. Firma, która funkcjonuje w Polsce, ale również w Dubaju, Nowym Jorku, Szwajcarii. Funkcjonuje mówię tutaj ma biura, bo przypuszczam, że pracujecie w znacznie większej ilości, dla znacznie większej ilości klientów z całego świata. Jak duży jest Wasz zespół? Czym się tak naprawdę zajmujecie?

Paula Januszkiewicz: Tak naprawdę to zajmujemy się, to ja może najpierw od tego zacznę, kilkoma rzeczami. Po pierwsze, projektami typu Incident Reponse, czyli jeżeli właśnie tak, jak właśnie wspominałam, klient jest zhakowany, no to naszym zadaniem jest pojechać on side, jak to mówimy i dokonać analizy, pomóc w odtworzeniu, postarać się na przykład zidentyfikować problem.

[00:05:09]

Paula Januszkiewicz: Czasem jest tak, że po prostu nie wiem, hakerzy są w danej sieci ciągle i naszym zadaniem jest zidentyfikowanie generalnie zakresu problemu, zakresu tego ataku też. I na przykład Forensiciem, czyli coś, co po polsku nazywa się informatyka śledcza. Natomiast ja wolę akurat określenie Forensic, bo mimo że być może to znaczy to samo, dla mnie Forensic często nie oznacza po prostu jakiegoś tam śledztwa, tylko po prostu dowiadywaniem się, dochodzeniem. Na przykład na

potrzeby klienta bez żadnych na przykład oficjalnych zgłoszeń do lokalnych oddziałów CERT, do Policji i tak dalej, co się tak naprawdę wydarzyło. Nie każdy ma ochotę przeprowadzać jakieś oficjalne śledztwo, ale na przykład chce na własne potrzeby dowiedzieć się czegoś. Więc jakby Forensic dla mnie definiuje trochę większy zakres działania. I oczywiście pentestami, to jest coś, z czego ja wyrosłam, tak naprawdę zajmując się pentestami przez całe moje, całe moje funkcjonowanie w cyberbezpieczeństwie. Czyli de facto legalne hakowanie, dostawanie się gdzieś na zlecenie, testowanie wszelkiego rodzaju aplikacji na przykład, czy to mogą być aplikacje webowe czy generalnie cała infrastruktura zewnętrzna, wewnętrzna, patrzenie jak infrastruktura wygląda z punktu widzenia użytkownika. Plus do tego mamy ponad 200 napisanych narzędzi wewnątrz naszej, naszej firmy. No i tak to, tak to wygląda. A jeśli chodzi o zespół, no to zależy oczywiście jak liczyć, tak. Bo mamy bardzo dużo osób, które z nami współpracują na stałe na przykład, więc my tak generalnie mówimy, że nasz zespół to jest ponad 40 osób, właśnie podzielony tak naprawdę i umiejscowiony na całym świecie. A to gdzie jesteśmy w kontekście biur, no to też tak jak słusznie wspomniałeś, nie ma tutaj znaczenia. Niemniej jednak oczywiście ma znaczenie z punktu widzenia lokalizacji, tak. Wiadomo, że klienci na przykład amerykańscy będą woleli współpracować z firmą w Nowym Jorku. Szwajcaria jest, akurat ja uwielbiam Szwajcarię, jest też bardzo specyficznym miejscem, dlatego że dużo klientów ze Szwajcarii właśnie chce współpracować z firmami tylko i wyłącznie ze Szwajcarii. Dubaj jest też specyficzny poniekąd, bo kraje właśnie JCC mają czasami takie wewnętrzne obostrzenia w kontekście firm, że chcą współpracować tylko i wyłącznie właśnie z, z firmami, które są z regionu JCC, czyli nie tylko Emiraty tak, ale też Oman i tak dalej, Bahrajn. Więc, więc generalnie rzecz biorąc, dlatego tak to wygląda, tak. A, a Polska oczywiście też jest, mamy tutaj największy zespół i współpracujemy Polską też z całym światem, więc tak jak, no można powiedzieć, że cyberbezpieczeństwo nie ma granic.

Prowadzący: Paula, przechodząc już do tematu naszego dzisiejszego odcinka, czyli – kilka kroków przed hakerem, często jest to takie powiedzenie, które jest odbierane, jako takie mocno sztampowe, tak. O ile oczywiście możemy się często chronić przed wieloma kampaniami, biorąc pod uwagę tak naprawdę nie wiem, czy to zdrowy rozsądek połączony na przykład z security awareness, gdzie użytkownik tak naprawdę, no może ominąć ten podejrzany link, może nie pobierać danego pliku. Ale znowuż z drugiej strony, często słyszymy, że mając po drugiej stronie tak naprawdę do czynienia z takim atakiem, no stricte targetowanym, uderzającym w dane organizacje, nie mamy szans. Możemy ewentualnie nie wiem, przeszkadzać czy opóźniać. Jak Ty uważasz? Jak to wygląda z Twojej perspektywy?

Paula Januszkiewicz: Wiesz, ja zawsze uważam, że jeżeli cały Internet będzie przeciwko nam, no to nie mamy szans. I, i to trochę też dotyczy na przykład właśnie ataków typu Denial of Service, gdzie generalnie duże organizacje mają jednak bardzo dobre zasoby, które mają za zadanie właśnie odebrać ten atak. Nawet nie w jakiś sposób temu zapobiegać, bo często ciężko zapobiegać na przykład właśnie

atakom typu Denial of Service, ale generalnie mają możliwość na przykład zwiększenia zasobów ad hoc. Na przykład nagle się okazuje, że infrastruktura staje się, na przykład z wykorzystaniem chmury, trzy razy większa, no i tak – to kosztuje. Niemniej jednak jakby cały czas są w stanie utrzymać odpowiadanie na ten ruch. No i po drugiej stronie znowuż, generowanie takiego ruchu też kosztuje tak, też wymaga organizacji, też nie może trwać wiecznie. Więc generalnie to jest też taki, taki ciekawy, ciekawy świat, bo jeżeli faktycznie takie ataki są bezpośrednio w nas wymierzane, tak naprawdę ciężko jest im w jakiś sposób zapobiegać.

[00:10:03]

Paula Januszkiewicz: Chociażby dając taki przykład, że jak się robi pentest i wchodzi się do infrastruktury, czy na przykład robi się właśnie pentest zewnętrzny, no to mamy jakiś ograniczony czas na wykonanie tych testów, tak. Powiedzmy jest to tam dwa, trzy tygodnie, czasami tydzień, w zależności od ilości pracy. Natomiast to też jest takie przeskalowane w kontekście minimalizowania ryzyka, więc jeżeli ktoś ma czas, no to spędzi z tą infrastrukturą i pół roku, tak. I okazuje się, że uda się komuś uzyskać dostęp i stąd też takie ataki na przykład pokazują się w mediach, że wiesz, jakieś znane firmy, ogromne firmy, gdzie moglibyśmy się nie spodziewać, że coś tutaj nastąpi, jednak taka firma została zaatakowana poprzez jakieś teraz, z naszego punktu widzenia, błahy błąd. Na przykład tak jak ostatnio było w Solar Winds z tym prostym hasłem, tak. Więc to są takie rzeczy, o których się dowiadujemy po czasie i myślimy sobie ha ha ha, my byśmy im czegoś takiego nigdy nie zrobili. No, jeżeli mamy infrastrukturę, która mieści w sobie kilka, kilkanaście, dziesiąt tysięcy użytkowników, no to ciężko zapobiegać tego typu sytuacjom. Czasami jest to po prostu kwestia przypadku.

Prowadzący: No właśnie, to może teraz przejdźmy do tego czynnika ludzkiego, o którym no ciężko zapomnieć. Czy jeżeli chodzi o użytkownika końcowego, który przez właśnie nieuwagę może stać się początkiem końca, czy to na przykład przez nieuwagę czy zaniedbanie administratora danego systemu, o czym też właśnie wspominałaś, czy w takich wypadkach security awareness to wszystko, co możemy zrobić, jeżeli chodzi o edukację tych ludzi? Na razie specjalnie chciałbym pominąć kwestię może właśnie związane z infrastrukturą bezpieczeństwa, a pozostać przy takiej, no stricte naturze ludzkiej.

Paula Januszkiewicz: Oczywiście. Tak naprawdę, tak. Więc, więc jeżeli na przykład mamy użytkowników, którzy są świadomi tego, w jaki sposób to zagrożenie w ogóle może wyglądać, skąd mogą być świadomi tylko i wyłącznie przez edukację, to będą w stanie wiedzieć, w jaki sposób przeciwdziałać, co zrobić, że na przykład, jeżeli dostaje maila, który nie wygląda dobrze, forwarduje go do IT. Jakby są w stanie zidentyfikować, że coś tutaj nie do końca pachnie dobrze. Więc im więcej takich programów edukacyjnych, ale też i dobrze zrobionych programów edukacyjnych, tym oczywiście lepiej. I widzimy, szczerze powiedziawszy ciekawe, że o tym wspomniałeś taki trend trochę wśród naszych klientów, że nasi klienci zaczynają zamawiać coraz częściej od nas właśnie programy związane z

cyberbezpieczeństwem i budowaniem świadomości wśród użytkowników. I niedawno realizowaliśmy taką bardzo dużą kampanię dla jednego z banków i tutaj było milion nagranych filmów, różnego rodzaju podcasty też i, i jakby forma dostarczania wiedzy jest bardzo zróżnicowana. Ktoś sobie może jechać samochodem i lepiej mu będzie posłuchać, ktoś woli oglądać filmik, ktoś na przykład lubi czytać artykuł, ktoś lubi na przykład samo demo. Więc jakby my staramy się tutaj absolutnie tak klasycznie, bym powiedziała podejść do tematu, czyli różnicować formy dostarczania materiałów. Ale bardzo istotny jest to czynnik, jeżeli chodzi o przeciwdziałanie atakom.

Prowadzący: No dokładnie, bo tak jak mówisz, z jednej strony kwestia tego, aby zainteresować tego użytkownika, żeby on rzeczywiście nie zrobił na zasadzie – dalej, dalej, dalej, test został zaliczony. A z drugiej strony chyba też właśnie to, o czym wspominałaś, czyli w jakość tych materiałów, bo ja się też nieraz spotkałem z takimi szkoleniami można to nazwać, gdzie na przykład kwestię związaną z phishingiem, no to było raczej na zasadzie – no nie odbieramy podejrzanych maili, rzeczywiście robimy forward do, do IT, nie klikamy w linki. Natomiast wiesz, bez wskazania, co może być podejrzanego w danym mailu, no to chyba to nie do końca może zadziałać.

Paula Januszkiewicz: Tak, oczywiście. Jakby tutaj istotna jest możliwość rozpoznania zagrożenia. Ale, co jest trudne tutaj to, to, że jeżeli na przykład dany phishing mail przejdzie przez filtry, które zakładam dana organizacja ma, no to, to oznacza, że ten mail phishingowy jest w jakimś tam stopniu dobrze utworzony, dobrze napisany. I tym trudniej użytkownikowi rozpoznać coś takiego, bo jeżeli automat nie rozpoznał, no to ten phishing mail przechodzi przez tę, przez tę barierę. Użytkownik ma całkiem ciężkie zadanie tutaj, bo ma za zadanie po prostu nie zareagować na, na takiego maila. Dlatego też bardzo istotnym faktem jest coś, co ja lubię nazywać kontekstem bezpieczeństwa albo kontekstem cyberbezpieczeństwa. Czyli generalnie po prostu kontekst naszej pracy, kontekst tego, z czym mamy na co dzień do czynienia, czy ja się spodziewam tego typu wiadomości, czy na przykład Anna, John pisze do mnie na co dzień takim językiem. Bo też może być tak, że na przykład konto kogoś, jakiegoś współpracownika zostało w jakiś sposób zhakowane, było na przykład proste hasło – tam i ten atak właśnie się zaczyna poprzez komunikację wewnętrzną z pracownikami, co kompletnie zmienia tutaj wymiar phishingu, tak.

[00:15:08]

Paula Januszkiewicz: Bo to są już phishingi, które są realizowane bezpośrednio z kont pracowników danej firmy. Albo też ktoś pisze z prywatnego konta. Także tutaj wiesz, takich sytuacji, punktów wejścia jest bardzo dużo. Niemniej jednak użytkownik, będący tym, który na koniec ma gdzieś tam kliknąć w link albo podać wręcz jakieś dane, bo to jest największe zagrożenie, musi przejść i regularnie przechodzić tego typu szkolenia, żeby zrozumieć, w jakim stopniu to może stwarzać zagrożenie dla organizacji.

Prowadzący: No dobrze. A jak z Twojego punktu widzenia infrastruktura może teraz wyprzedzać, właśnie wyprzedzać użytkownika i wspomagać pracowników danej instytucji? Bo ilość rozwiązań związanych z cyberbezpieczeństwem jest ogromna i będzie coraz większa, przypuszczam. Więc tutaj, w jaki sposób, jak, jak Ty widzisz te trendy? W jaki sposób można składać te klocki, aby stworzyć system, który no będzie taką podstawą tak naprawdę do dalszej, dalszej pracy i do dalszego bezpieczeństwa dla użytkowników końcowych?

Paula Januszkiewicz: Oczywiście mamy dostęp do technologii, która pozwala nam na zminimalizowanie ryzyka do stopnia, który jest absolutnie satysfakcjonujący z punktu widzenia bezpieczeństwa. Na przykład, na Windowsie 10 mamy dostęp do na przykład czegoś, co się nazywa ASR, czyli attack surface reduction rules. I to są takie reguły, które się konfiguruje w PowerShellu, bardzo proste, bardzo, bardzo proste do wdrożenia, które są wbudowane w system, wystarczy po prostu je włączyć. I one na przykład zapobiegają tworzeniu się child processu, czyli procesu potomnego, na przykład z makra excelowego, który użytkownik gdzieś tam sobie odpali, tak. Czyli na przykład, gdy użytkownik dostanie maila, jest tam excelek, ma makro, użytkownik klika enable makro i generalnie pod spodem uruchomi nam się kod. I ten kod jest tym kodem potomnym, procesem potomnym. No jakby to ten typ zachowania jest jak najbardziej nam znany, więc możemy go po prostu w bardzo prosty sposób zablokować. I to też, jakby rzadko się zdarza, że mamy do czynienia z legalnymi sytuacjami, które po prostu miałyby za zadanie w podobny sposób działać, tak. Czyli faktycznie, ktoś musiałby w firmie regularnie używać makr i wtedy taka reguła, no to nie miałaby znaczenia. Ale są też i inne reguły, które tutaj mają znaczenie typu sposób, w jaki nie wiem, piszemy po dysku, jakieś anomalia. Więc absolutnie mamy możliwość wykrycia nie tylko takich ataków, ale również zablokowania plus wiesz, wszelkie rozwiązania, teraz to też taki trend bazujący na machine learningu. Czyli na przykład antywirus, który korzysta z jakiejś centralnej bazy vendora, która na przykład zbiera patterny, zbiera wszelkiego rodzaju zachowania. I na przykład, jeżeli uruchamiany jest kod, który tam ma na przykład privilege DBA [niepewne], czyli pozwala na debugowanie procesów, który jednocześnie podpina się do procesu typu LSASS, no to najprawdopodobniej będzie to Mimikatz, czyli narzędzie do kradzieży tożsamości, tak w dużym skrócie opisując. I takie zachowania jakby będą też blokowane. Co na przykład samo DBA privilege, o którym mówiłam nie jest niczym złym. Bawienie się lsassem zależy tak, od sytuacji, bo na przykład Authentication providers mogą również być ładowane przez lsass, ale znowuż to nie jest typowe. I tak dalej. Jakby tych anomalii jest naprawdę dużo. No, ale właśnie po to jest machine learning, żeby przeciwdziałać czemuś takiemu. No i oczywiście exploit guard, czyli coś, co pozwala nam na przeciwdziałanie wykonaniu na przykład kodów w jakimś tam stopniu w pamięci tak, albo bezpośrednią modyfikację pamięci procesu. Czyli coś, czemu antywirus nie jest w stanie przeciwdziałać. Natomiast to jest taki obszar, w którym bardzo często realizowane są podatności. Czyli

mamy jakieś, jakieś, jakąś aplikację, jakiś proces, jakąś usługę, która jest na coś tam podatna, no i pytanie, w jaki sposób ta podatność może być właśnie zrealizowana. No poprzez jakiś tam szereg określonych funkcji, wywołanych w określony sposób. No i znowuż, to nie jest też rocket science, po prostu tych rzeczy jest tak dużo, że ciężko jest po prostu zamknąć wszystko i z niczego nie korzystać. I to by było w sumie dobre. Natomiast, no to nie jest zbyt użyteczne z punktu widzenia biznesu.

Prowadzący: Wiesz co, obiecywałem na samym początku, że poruszymy dzisiaj również kwestie związane z kilkoma raportami czy statystykami. I rzeczywiście w tym tonie chciałem teraz uderzyć. Pozostańmy przy tak zwanym TTD czy MTTD, czyli time to detect czy mean time to detect. Mnóstwo firm, szczególnie właśnie związanych z cyberbezpieczeństwem publikuje tego typu raporty, które wiesz, otwarcie mówią, jak dużo dni mija od włamania do jego wykrycia tak, w zależności od raportu. [00:20:09]

Prowadzący: No te wartości oczywiście mogą się różnić. Natomiast no gdzieś z reguły oscylują w okolicach 180 – 200 dni.

Paula Januszkiewicz: 200, mhm.

Prowadzący: Skąd tak duża wartość?

Paula Januszkiewicz: Ha ha. Mam wrażenie, że to jest troszkę problem naszych czasów i nawet nie tyle, że teraźniejszych, co trochę problem z przeszłości. Dlatego że w przeszłości, niedalekiej mieliśmy do czynienia z infrastrukturami, które nie stawiały nacisku na monitorowanie. I mamy na przykład dostępne wbudowane logi systemów operacyjnych, no i ok, super. Natomiast te logi bardzo często mają bardzo niewielki rozmiar typu 64MB, 32 MB i tak dalej. Tak jak w przypadku Windowsa mamy Event Log. W zależności od logu, no to mamy do czynienia z takim rozmiarem. Co w intensywności codzienne i codziennej pracy systemu taki log jest nadpisywany nad, nawet i czasami kilka razy dziennie. Więc skąd my mamy wiedzieć, że atak w ogóle nastąpił? Są mechanizmy w systemie wbudowane, które pozwalają nam na trochę analizy tego, co się wydarzyło, na przykład [niepewne] journal, czyli anti [niepewne] journal, czyli log zbierający informacje o transakcjach na systemie, w systemie plików. I to też jakby, czy to zostało uprzednio skonfigurowane? No powiedzmy, że nie, ale domyślnie też konfiguracja tego nie jest zła. No i tam mamy załóżmy nie wiem, 2GB danych tekstowych, które gdzieś pokazują nam, jakie pliki zostały w ogóle rzucone na dysk w czasie ataku. I też bardzo istotne jest powiedzenie tego, że 200 dni przykładowo no to, to jest ten czas, który zdecydowanie pozwala nam na nadpisanie wielokrotne, tego typu logu również. Mamy na przykład w Windowsie Prefetch, czyli usługę, która tam wspiera, powiedzmy w dużym skrócie wydajność systemu i sposób ładowania się procesów. Niemniej jednak Prefetch ma taki back up, jeżeli chodzi o funkcjonalność, właśnie w postaci nagrywania, monitorowania tego, co się w ogóle uruchamia. No i tutaj akurat Prefetch akurat ma tę zaletę, że on jest zawsze ważny. Więc jak sobie zainstalowaliśmy tam system

dwa lata temu, no to Prefetch będzie uwzględniał właśnie rzeczy sprzed dwóch lat. I zajmuje tam 100MB na dysku, więc absolutnie nieistotne. Więc jakby to są takie główne rzeczy. No jeszcze usługa indeksowania tak, ale też niezbyt, niezbyt można na niej polegać. To są takie rzeczy, które są w system wbudowane. I teraz, co jeszcze? No i jeszcze mamy na przykład rozwiązania i to już mówimy o rozwiązaniach zewnętrznych, tak. Czyli na przykład Sysmon, który jest za free. Więc jakby to oznacza, że ktoś musiał skupić się na tym, co tak naprawdę w takiej infrastrukturze jest potrzebne, jak nie tylko monitorować, bo to akurat żadna sztuka, ale i również jak zbierać, i analizować, i interpretować te logi, w jakiś sposób ustawić sobie takie treasures. Takie punkty, które powiedzą nam, czyli generalnie alarmy tak, alerty, które powiedzą nam, że coś w ogóle tutaj się wykonało nie tak jak trzeba albo ten proces, który się właśnie uruchomił jest nieznany, albo ten użytkownik, on się zwykle do tego serwera nie loguje. No to tutaj już mówimy o takiej w miarę zaawansowanej interpretacji tych logów. Więc to wymaga wdrożenia centralnego systemu zarządzania logami, zasubskrybowania się do tych logów po stronie serwerów i stacji. Więc ja bym powiedziała, że to jest domyślne zachowanie, które każda infrastruktura i domyślne podejście, które każda infrastruktura powinna wdrożyć, mieć. Niemniej jednak stosunkowo niedawno nie mówiliśmy o tym. Cyberbezpieczeństwo nie było popularne tam w dwa tysiące, powiedzmy nawet i 2018, 2019 to był ten taki czas trendu, kiedy ludzie zaczęli o tym mówić, zaczęli wchodzić w te rozwiązania. Teraz mamy tych rozwiązań, tak jak mówiłeś całą masę. Ale wcześniej nie mieliśmy do czynienia z czymś takim, był splung, był QRadar [niepewne] i tak dalej. No i okej, tak jakby też nie każde firmy było na to stać, bo to są rozwiązania drogie, bardziej takie do enterprisów. Więc tutaj ta warstwa taka tych mniejszych i średnich firm w jakiś sposób nie była zaadresowana z punktu widzenia bezpieczeństwa. A, no nie ukrywajmy w Europie chociażby na ten przykład, dużo jest firm, które mają średni rozmiar. I, i stąd też mamy do czynienia z sytuacjami, gdzie to bezpieczeństwo zostało gdzieś złamane tak, i my nie wiedzieliśmy, co w ogóle się wydarzyło. Więc to 200 dni, o których mówisz to też James Comey, były dyrektor FBI też bardzo często to podkreślał, że 200 dni to jest właśnie ten czas, a 80 dni jest potrzebne danej firmie, żeby w pełni się odtworzyć. [00:25:11]

Paula Januszkiewicz: Bardzo droga operacja, bo to oznacza, że mamy dodatkowych konsultantów przez 80 dni. No, ale cóż, jakby dokładnie też to jest to, co ja widzę. Powiem Ci, że na przykład jak idziemy do infrastruktury, coś tam widzimy, okej, jest jakiś atak, no i na przykład widzę, że w ogromnej instytucji sub rządowej finansowej takiej, że naprawdę nie chcemy widzieć tej organizacji zhakowanej okazuje się, że hakerzy to siedzieli ponad rok. No, więc wiesz, jakby nie przeraża mnie ta liczba, ale jednocześnie obiektywnie fajnie by było, jakby to było zero dni, bo te ataki się nie wydarzyły. Ale też z innej strony jest to pozytywna liczba, bo przynajmniej się dowiedzieliśmy, że jest to 200 dni.

Prowadzący: Ale wspominasz o najróżniejszych systemach, które mogą wspomagać, mogą tak naprawdę monitorować infrastrukturę. No, ale jeszcze pozostaje kwestia osób, które no muszą przy tych systemach siedzieć.

Paula Januszkiewicz: Tak, ale też i jeżeli dobrze systemy są ze sobą połączone i dobrze są skonfigurowane właśnie te obszary do zmonitorowania, do monitorowania, no to tym mniej tych osób powinno siedzieć. Ale oczywiście istnieje idea SOC, który, czyli security operation center, który ma za zadanie tak naprawdę monitorowanie tego i reagowanie na to, co te systemy nam wyświetlą. To w takim bardzo dużym skrócie. Oczywiście są i prostsze zadania, i absolutnie dużo trudniejsze zadania. Natomiast rolą SOC generalnie jest właśnie wykrywanie tego typu zagrożeń.

Prowadzący: Wiesz co, skoro już wspomniałaś o FBI, to chciałbym przytoczyć jeden raport, Internet Crime Report FBI z 2020 roku. Dane, które są tam przedstawione opisują między innymi ilość rzeczywiście incydentów, ale również właśnie koszty związane z tymi incydentami. I raport ten pokazuje, że ilość incydentów w latach bodajże 2016 – 2020 w USA zwiększyła się o około 265%. To samo tyczy się strat finansowych z tym związanych w tym samym okresie, był to przyrost o około 280% i kwota przekraczająca 4,2 mld dolarów. Jak w tym wypadku wyglądają te przeliczniki? I skąd też biorą się tak wielkie kwoty? I pytam nieprzypadkowo, bo, bo często wydaje mi się, że to taka troszkę gra mająca na celu z jednej strony zastraszenie instytucji. Ale z drugiej strony, czasami wystarczy się zastanowić nad kosztem kilku godzin postoju jakiejś fabryki, aby zdać sobie sprawę z powagi tej całej sytuacji. I, że rzeczywiście jesteśmy w stanie spokojnie się zbliżyć do, do tak dużych kwot, strat, jeżeli chodzi o firmy.

Paula Januszkiewicz: Jasne. Już wyjaśniam, z czego takie kwoty wynikają. Plus ciekawe, że przytoczyłeś ten raport FBI, bo on też mówi, że właśnie ataki w zależności tam od, od czasu. Generalnie w czasie tam pandemii oni też to podsumowali, że wzrosły te reported attacks, oni przytoczyli te, o których oni wiedzą.

Prowadzący: [Niepewne].

Paula Januszkiewicz: Dokładnie. Czyli o tą, o tą właśnie tam prawie właśnie 300%. No to generalnie, generalnie rzecz biorąc te koszty biorą się z kilku rzeczy. Po pierwsze, przestój w operacji. I na przykład przywołując przykład z życia wzięty, niedawno mieliśmy przyjemność uczestniczyć w projekcie na żywo w Niemczech o międzynarodowej organizacji, która została właśnie zhakowana. Ich dane zostały zaszyfrowane, zostali poproszeni o zapłacenie okupu, czyli klasycznie ransomware, gdzie ich akurat wyniósł ten okup i zapłacili go – kilkaset tysięcy euro. Nie mówiąc już o kosztach, które są związane z zatrudnieniem właśnie tak jak wspomniałam konsultantów plus cała organizacja z tym związana, plus przestój. Tak, więc jakby tutaj te koszty, one pięknie się mnożą w kontekście, w kontekście takiego ataku. Jak jest dobrze, to jest dobrze, a jak jest atak, no to niestety i być może kwestia okupu dochodzi,

i kwestia dodatkowych konsultantów, i kwestia przestoju, i potem kwestia edukacji użytkowników. Więc jakby wszystko tutaj ma znaczenie. Więc stąd, każdego typu przestój jest absolutnie, absolutnie drogi. Ale też i nie tylko ransomware generuje nam ogromne koszty, bo też kiedyś miałam przyjemność uczestniczyć w innym projekcie, gdzie administrator, czyli osoba zatrudniona przez daną organizację była, był trochę sabotażystą i wyłączał poszczególny komponenty infrastruktury, a potem generalnie wchodził i powiedział – O, ja tu chyba wiem, co się wydarzyło, ja to naprawię. No i wszyscy oczywiście go bardzo kochali, on był wspaniały, najmądrzejszy, dostawał premie. Więc on generował problem, on go naprawiał.

[00:30:01]

Paula Januszkiewicz: I kiedyś wygenerował tak ogromny problem, że cała tutaj fabryka była właśnie offline przez 2,5 dnia. I oni straty przez ten czas określili na około 4 mln euro, więc całkiem sporo. I to akurat zmotywowało tą organizację właśnie do przeprowadzenia dodatkowych testów. No ja byłam tą osobą, która była on side. I miałam za zadanie dociec w ogóle, co tam się wydarzyło, bo oni zauważyli taką tendencję, że coś, co jakiś czas się dzieje i to jest w ogóle bez kontekstu. I generalnie, no i właśnie się okazało, że to był ten administrator. Więc nawet i tak proste rzeczy powodują koszty, czasami te koszty są bardzo ciężkie do wyliczenia. No, bo, no okej jakby, jeśli fabryka stoi przez tam 2,5 dnia no to, to jest jasne tak, ale dodatkowo jeszcze jest ransomware, dodatkowo są jakieś koszty konsultantów, więc generalnie oczywiście na koniec można to podsumować, no i wychodzą absolutnie ogromne koszty. Więc łatwiej jest zapobiegać. A co mnie zawsze zastanawia, bo organizacje mówią – A nie, my nie mamy budżetu na cyberbezpieczeństwo. Czasami jak bierzemy udział słuchaj, w jakichś przetargach, no to się nagle okazuje, że, co nie mówię, że to jest złe tak, ale, że cena ma znaczenie, ale takie pierwszorzędne, takie priorytetowe. Że im tańszy projekt cyberbezpieczeństwa…

Prowadzący: Tak, rzeczywiście.

Paula Januszkiewicz: Tym lepiej, tak. I, i mnie to przeraża, bo w cyberbezpieczeństwie ogromną rolę odgrywa jakość. Cena jak najbardziej też, ale przede wszystkim jakość. I jak można wierzyć organizacji, która czy tam firmie, która będzie testowała jakąś inną organizację, jeżeli ona jest ekstremalnie tania. Coś tu jest nie tak. Żeby się nauczyć dobrze operować tymi wszystkimi narzędziami, teoriami, pojęciami, w ogóle systemami w cyberbezpieczeństwie naprawdę trzeba sporo w siebie przede wszystkim zainwestować, czy pracownik musi gdzieś uczestniczyć w szkoleniach. Firmy consultingowe naprawdę sporo wydają na pracowników, jeżeli chcą, żeby oni byli dobrzy w tym, co robią. I przede wszystkim czas, który dana osoba musi poświęcić na nauczenie się tego. To też nie jest za darmo, tak. Przepraszam, że tak pragmatycznie podchodzę do tego, ale ja u siebie zatrudniam osoby, więc ja wiem jak to wygląda. I na koniec, to nie może być super tanie. To jest coś podejrzanego w tym. To może być, mieć okej cenę, ale nie być super tanie. No i później…

Prowadzący: To wszystko musi być skalkulowane. To jest sprawa jasna.

Paula Januszkiewicz: Dokładnie. Później, czego się spodziewać, tak – my byliśmy przetestowani, a jednak nas zaatakowali. No, no tak, no.

Prowadzący: A słuchaj, a jak wygląda sytuacja w Polsce? I czy te wartości, z tych krajów zachodnich mogą być w pewien sposób mapowane również na nasze podwórko?

Paula Januszkiewicz: Jak najbardziej mogą i powiem Ci, że ja to w ogóle nie jestem fanem porównywania się do zachodu, tak. My jesteśmy zachodem albo wręcz jesteśmy centralną Europą, to powinno nas czynić jeszcze bardziej dumnym z tego, z tego, kim jesteśmy. Bo powiem Ci, że Polacy akurat i polskie firmy, bywa różnie, ale jeżeli ktoś faktycznie o to dba, to dba o to na maksa. I ja uważam, że polskie firmy często powinny na przykład, powinny stanowić wzór właśnie dla zachodnich organizacji. Bo często jest tak, że na przykład nie wiem, jak mamy projekty, bo mamy bardzo dużo projektów w każdych miejscach na Ziemi, dosłownie i to wszystko też zależy od budżetu. Bo jeżeli dana organizacja ma budżet, to akurat Polacy, też nie chciałabym uogólniać w żaden sposób niczego tak. Ale mają też taki, takie podejście, że – ok, mamy ten budżet, no to musimy go wydać mądrze. I jak ktoś faktycznie serio do tego podchodzi, to tutaj jest bardzo dużo takich mądrych oszczędności porobionych, czasami aż za, za strict, za bardzo. Niemniej jednak, jakby widać, że rzeczy idą do przodu. A na przykład, jak uczestniczyłam właśnie niedawno w jeszcze innym projekcie na zachodzie, tak to nazwijmy, to się okazało, że dana infrastruktura została zaatakowana, dlatego że firma miała vendora, jakiegoś kontraktora, który zarządzał ich infrastrukturą, po części. I atak przybył z, właśnie od nich, z sieci tego kontraktora. I się okazało, że atakujący był Domain Adminem w danej organizacji, właśnie na koncie kontraktora. No i potem mini tam śledztwo, się okazało, że faktycznie tam tak było, tak. No i, co dalej, tak? Tak jakby oni mieli takie podejście, że przyszła godzina 16:00 i do domu, tak jakby priorytety się zmieniają, od 8:00 do 16:00. Bardzo ważna infrastruktura, ważna, atak straszny, wszystko straszne, trzeba się odtwarzać, szybko, szybko, szybko, a po godzinie 16:00 wszyscy jadą do domu. Więc u nas czegoś takiego nie ma. U nas jest tak, że jeżeli się pojawia zadanie, to my podchodzimy do niego z całym sercem i to jest coś, co ja bardzo lubię widzieć.

[00:35:03]

Paula Januszkiewicz: Ale też jest druga strona medalu. Nie wszystkie firmy niestety mają pieniądze na cyberbezpieczeństwo. I to niestety jest bardzo demotywujące. Więc te projekty się toczą zupełnie innym trybem.

Prowadzący: Tak. Czasami wystarczy rzeczywiście porozmawiać z administratorami takich firm, którzy są po prostu sfrustrowani czasami po prostu budżetem. I, i bardzo często w niewybrednych słowach to nawet są w stanie przekazać dalej. Słuchaj wiesz, co chciałbym wrócić jeszcze do tematu phishingu. Bo, bo tak jak rzeczywiście wspominaliśmy, Ty wspominałaś również ostatnio króluje on w różnych

raportach, w najróżniejszych odmianach i wzrost jest tutaj niesamowity. I mam do Ciebie pytanie. Czy z Twojego punktu widzenia wiąże się to z coraz lepszym przygotowaniem tego typu kampanii czy z popularną oczywiście ostatnimi czasy pracą zdalną, chwytliwym tematem? Bo też mówiąc wprost, nie tak dawno naprawdę nieźle się ubawiłem, że przestępcy wykorzystują tak naprawdę fake newsy związane z koronawirusem, jako [niepewne] po prostu, a tym samym są w stanie przejąć poświadczenie niczego nieświadomych, a żądnych sensacji i wiedzy ludzi.

Paula Januszkiewicz: Standard. W dzisiejszych czasach w ogóle wykorzystywanie takich trendów społecznych do phishingu, no to jest oczywiście gwarant sukcesu, tak. I, i też podejrzewam, i Ty, i Ty jak mielibyśmy za zadanie stworzyć kampanię phishingową, to byśmy się zastanawiali…

Prowadzący: Temat jest jasny. Oczywiście.

Paula Januszkiewicz: Dokładnie. Dokładnie. W co tutaj uderzyć? Uderzmy w jakiś taki słaby punkt, tak. Kiedyś nie było masek, był problem z zamówieniem masek, no to oczywiście tutaj dostajemy mail, że – tu można zamówić maski. No to wiadomo, jakby tutaj działamy na emocjach zawsze. Działamy też i na przykład na takich typowych cheatach związanych z relacjami między pracownikami. Na przykład my często, jako firma dostajemy na przykład taki phishing, że ktoś do nas pisze i mówi, że – Paula Januszkiewicz powiedziała, że można.

Prowadzący: To jak szef mówi, że można, to można. No i nawet trzeba.

Paula Januszkiewicz: To można. A nawet dokładnie, trzeba. Więc, więc też jakby wiadomo, że ja się tak nie komunikuję z nikim i pytanie, kim jest ta osoba w ogóle? Więc my to wiemy, tak. Ale też, też to są takie zabawne próby, które niestety w dużych organizacjach mogą zadziałać, tak. Bo ktoś może mieć organizację, gdzie pracuje 100 tysięcy osób, tak i ja nie znam Johna, który do mnie pisze, ale znam mojego szefa. I tak dalej. Także absolutnie, absolutnie trend teraz. No i cóż, jakby im bardziej uderzamy tak jak już mówię, mówiłam w emocje, tym większe szanse na sukces.

Prowadzący: Kolekcjonujesz sobie takie najlepsze artefakty, które do Ciebie trafiają, jeżeli chodzi o tego typu wiadomości?

Paula Januszkiewicz: Czasem, czasem tak, jak coś jest naprawdę fantastyczne. Ja to lubię też takie śmiechowe rzeczy tak, typu księżniczka tam z South Arabia mówi, że nie ma co zrobić z 1 mln dolarów i – proszę, pomóż. Więc…

Prowadzący: Nie złotem? Tym razem to nie złoto, tym razem to już gotówka po prostu była?

Paula Januszkiewicz: Wezmę i to, i to.

Prowadzący: Słuchaj, ale rzeczywiście czasami poradzenie sobie z phishingiem, no jest mocno rzeczywiście problematyczne. I tutaj wracając do też początku naszego, naszej rozmowy, na co tak naprawdę z Twojej perspektywy należy zwracać uwagę? Co powinno powodować zapalenie się u nas takiej ewidentnie wiesz, czerwonej lampki? Nie mówię tutaj o wiadomościach, które są powiedzmy nie

wiem, ewidentnie wrzucone na gogle translate tak, i w takiej mówi łamanej polszczyźnie do nas, gdzieś tam przerzucone. Tylko, co, na co najlepiej użytkownicy szczególnie, powiedzmy nietechniczni powinni też zwracać uwagę?

Paula Januszkiewicz: No kilka rzeczy tutaj mamy. Na przykład właśnie ten kontekst przede wszystkim, który definiuje nam nasz, nasze stanowisko pracy. Czasami on jest jednak naruszony. Przykładowo, kiedyś byłam na projekcie w takim, z technologii kosmicznych, tak to nazwijmy, w Hanceville [niepewne] w Alabamie, wynajęłam samochód z Avisa, oddaję go na lotnisku i zaraz po tym dostaje maila, czyli kontekst jest, że – hej, hej, znajdź tutaj, proszę find requested rental receipt. I generalnie, tak sobie myślę – halo, halo, ja nie prosiłam o żaden rachunek tak, a oni mówią mi, że jest requested. To po pierwsze. Drugie, logo Avisa było takie trochę zblurowane, czyli skompresowane, też dziwne. Nikt nie powiedział mi – Hallo Paula czy tam w ogóle – Hallo albo coś w tym stylu, więc też dziwne. Czcionka była taka trochę mix, czyli różne czcionki były w mailu. Temat też nie do końca mi siadł, bo było Avis tam rental i było cases, czyli wiele spraw, a nie jedna plus za dużo spacji w tytule. Pamiętam, bo jakby to absolutnie zwróciło moją uwagę. No i tam w środku był pdf. I co się okazało, ten pdf w ogóle był mały, bo on miał kilka KB, co jest też nietypowe dla pdfa, pdfu.

[00:40:01]

Paula Januszkiewicz: I otworzyłam tego, ten plik, ten załącznik później u siebie, takimi narzędziami do analizy pdf. I się okazało, że właśnie ten pdf wykorzystywał podatność Adobe [niepewne] na tamten czas, gdzie, jeżeli kliknęłabym gdziekolwiek w tym pdf, gdziekolwiek, to to by spowodowało nawiązanie połączenia typu [niepewne] shell do jakiejś konsoli hakera, który gdzieś tam sobie czekał, tak. Więc to tak kiedyś, z przeszłości, tak. Więc kontekst był. No i, ale też i były inne czynniki, które sprawiły, że absolutnie ten phishing, no stał się phishingiem w efekcie, w moich oczach. Właśnie typu tytuł, typu, z jakiego maila to przychodzi, typu, w jaki sposób jest to sformatowane. Plus też fakt, że ten plik jest duży, mały, on zawiera to makro. Ten pdf akurat to była bardzo specjalna sytuacja. Czasami też i możemy to zweryfikować z naszymi znajomymi. I im więcej się mówi, tak swoją drogą na ten temat bardzo istotny czynnik rozpoznawczy, jeżeli chodzi o phishing, gdy rozmawiamy ze znajomymi, z współpracownikami, z IT i tak dalej, tym lepiej. Bo może ktoś inny też doświadczył tego typu sytuacji i mówi – no faktycznie, ja też zostałem takiego maila, może nie klikaj lepiej w to tak. Jakby to, tutaj ten moment zawahania zawsze powinien przemawiać za – nie, nie rób tego. I to jest coś, co na przykład my tłumaczymy użytkownikom w kontekście właśnie tego security awareness – jeśli się wahasz, to nie. No i oczywiście w nadziei, że rzeczywistość będzie tożsama z naszymi emocjami, z odczuciami. Jeżeli jest inaczej, no to mamy fail.

Prowadzący: Tak. Ja przynajmniej też apeluję do firm, które zamawiają tego typu szkolenia, żeby zwróciły uwagę, żeby jak najwięcej rzeczywiście tych przykładów było. A to, co mówisz, jeżeli nie mamy

pewności zawsze lepiej zgłosić to do odpowiedniego działu, zamiast po prostu bezmyślnie, bezmyślnie klikać. Paula, oglądałem wiele Twoich wystąpień, ale chciałbym przytoczyć jedno, które myślę, że bardzo dobrze wpisuje się w dzisiejszy temat. Twoje wystąpienie na konferencji RSA – Think and Act Like a Hacker to Protect Your Company's Assets. I nie będę ukrywał, że na początku po prostu naprawdę kładłem się ze śmiechu biorąc pod uwagę Twoją opowieść, jak wykorzystując tak naprawdę ludzkie odruchy można się w łatwy sposób dostać do wielu, wielu miejsc. Czy często zdarza Ci się w taki sposób przenikać rzeczywiście do organizacji Twoich klientów?

Paula Januszkiewicz: Dzięki przede wszystkim, że znalazłeś czas na obejrzenie sesji. Tak, mówisz o historii z windą, która jest moją ulubioną historią.

Prowadzący: Tak, o Twojej historii z windą.

Paula Januszkiewicz: Dokładnie. Często, absolutnie często, w zasadzie to za każdym razem tych historii jest cała masa i one czasami mają taki ciekawy właśnie kontekst. Czasami mamy jakiś tam nastrój na pociągnięcie właśnie tych historii trochę dalej, tak jak właśnie ta historia, o której wspominasz. A czasami po prostu są to takie proste wejścia tak, jakby zero romantyzmu, po prostu gdzieś tam wchodzisz do danej organizacji i się okazuje, że jest to absolutnie proste. I takie ataki, mówimy tutaj o inżynierii socjalnej, one bardzo często niosą ze sobą kolejny etap, że na przykład ktoś, komu udaje się już być w tej infrastrukturze, więc wchodzi teraz technologia. I na przykład używamy tych pendrivów, tak. Idziemy, patrzymy, kto nie zablokował laptopa. Ewentualnie gdzieś w jakiś sposób eskalujemy się dalej, tak. Więc podrzucamy komuś tego pendriva, więc jakby tutaj tych sytuacji jest masa i na pewno musimy być na nie uczuleni. A tak naprawdę, jeżeli chodzi o ilość i jakby ten współczynnik tego, że coś się nie udało, a coś się udało. Tylko raz mi się nie udało, a poza tym to się udało. Więc nawet nie jest to 99.999 tylko 999% się udało.

Prowadzący: To jak w takim razie z Twojej perspektywy wyglądają takie best practices dla organizacji oczywiście, nie mówię dla Ciebie?

Paula Januszkiewicz: Znowu kontekst. Czyli na przykład, jeżeli ja sobie siedzę przy biurku, widzę, że ktoś się kręci, nie znam tej osoby, to nie wstydzę się powiedzieć – kim Ty jesteś? Nie wstydzę się zagadać, nie wstydzę się nawiązać nawet i takiej prostej rozmowy, która nie jest jakąś rozmową przepytującą, tylko jakimś zagadaniem o coś, tak i zobaczeniem jak ta osoba reaguje. I wtedy wybadanie tej sytuacji. Wiadomo, że nie każdy tutaj będzie psychologiem i będzie w stanie rozpoznać być może świetnie wyszkoloną osobę, która, z którą właśnie mamy do czynienia, tak. Ale generalnie to jest coś, co być może spowoduje, zminimalizuje ryzyko ataku i spowoduje, że taka osoba w naszych oczach będzie się jawiła, jako właśnie podejrzana. No i wtedy dalej wyeskalować taką sytuację. Na pewno pracownicy muszą wiedzieć, w jaki sposób dalej eskalować tę sytuację, do kogo zadzwonią, tak. [00:45:02]

Paula Januszkiewicz: Na ochronę, potem się okaże, że się nie dodzwonią. Tak jakby musi być ścieżka zaopiekowania się tematem.

Prowadzący: W końcu wpuszczą – dobrze, to pani sobie idzie.

Paula Januszkiewicz: Dobra, dokładnie, dokładnie. Tak i tak właśnie, tak jest.

Prowadzący: A czy to nie jest troszkę tak, że czy to właśnie, jeżeli chodzi o taki typowy social engineering na miejscu, czy jeżeli chodzi właśnie o te kampanie, że my troszeczkę zbyt zawierzamy czasami systemom i całej otoczce, którą wokół wiesz cyberbezpieczeństwa często rozsiewają właśnie działy IT? Że mamy swoje procesy, mamy swoje procedury, mamy system A, B, C, D i tak dalej. To nie jest tak, że troszeczkę za bardzo zawierzamy?

Paula Januszkiewicz: Zawierzamy, to tak wydaje mi się jest. Z drugiej strony czasami możemy być nieświadomi w tym zawierzaniu, co tak naprawdę pod spodem się kryje. Bo sam atak na przykład jest skomplikowanym procesem. I czy jesteśmy w stanie omijać systemy bezpieczeństwa? Oczywiście. Wiedząc jak one wyglądają, chociażby taki przykład takich klasycznych antywirusów, omijanie ich jest mega proste. Z racji tego, że jakby one działają na określonych zasadach, typu na patternach, na jakichś zachowaniach. Więc wystarczy stworzy swoje nowe zachowanie jakiegoś procesu, jakiegoś oprogramowania i jeszcze parę innych technik i się okazuje, że w ogóle antywirus nie wykrywa czegoś, co jest po prostu mega, mega złośliwe, tak. Więc zawierzamy, a z drugiej strony wiesz, też trochę nie mamy wyjścia, bo co możemy zrobić innego, możemy wdrożyć więcej systemów. Możemy wdrożyć znowuż jakieś lepsze praktyki monitorowania. I zawsze to będzie więcej i więcej, kończąc na koniec, kończąc w sytuacji, w której tych systemów będzie tyle, że po prostu komfort naszej pracy będzie tym bardziej powodował problemy. Więc gdzieś musimy tutaj znaleźć złoty środek i niestety nawet w cyberbezpieczeństwie niestety istnieje koncept zaufania. Chociażby ufamy Root CA, czyli wydawcom certyfikatów, co też kiedyś pokazało parę problemów. To tak, nie to było problemem tylko generalnie ukradzione klucze były problemem. Ale tak czy inaczej zawsze ten kontekst się gdzieś tam pojawia. Więc musimy sobie określić taki idealny stan, w którym powiemy – okej, na dzień dzisiejszy przez najbliższe 3 miesiące używamy tego w taki sposób tak, a potem weryfikujemy swoje podejście.

Prowadzący: Słuchaj, jakie grzechy główne instytucji mogą być właśnie na przykład otwartymi drzwiami dla napastników? Ty bardzo często powtarzasz o kwestiach związanych właśnie z hasłami i kwestiach związanych z inżynierią, z PowerShellem, [niepewne], oprogramowania. Co najczęściej tutaj może być takim głównym grzechem instytucji?

Paula Januszkiewicz: Najgłówniejszym grzechem będzie mały, za mały budżet na cyberbezpieczeństwo. Więc generalnie tutaj trzeba by się zastanowić, jak powinna wyglądać w ogóle ta nasza cybersecurity posture, ten nasz obraz cyberbezpieczeństwa, strategia cyberbezpieczeństwa w organizacji i ile to w ogóle będzie kosztowało. Jak nas nie stać i jak wygląda nasz roadmap, jak wygląda

nasz plan wdrożenia, na ile lat to rozkładamy, jaki system wiążą ryzyka. Także największym grzechem jest po prostu brak planowania i niestety czasem budżetu w kontekście cyberbezpieczeństwa. Ale też jednym z takich istotnych problemów, który ja obserwuję to jest często sytuacja, w której organizacja myśli, że sobie świetnie radzi. I w ogóle takie określenia zawsze mnie trochę przerażają, bo co to znaczy? Względem czyich oczu, względem, jakich statystyk, względem, jakich systemów, tak? Więc jeżeli mamy coś na zielono, no to wcale nie znaczy, że sobie radzimy świetnie, tak. Więc to też akurat tak swoją drogą w kontekście tych krajów, o których mówiliśmy, jest dobrą bardzo cechą u Polaków, że pewnie się powtarzam też i po innych, ale my też tak trochę lubimy sobie ponarzekać, to dobrze. Akurat cyberbezpieczeństwo, to bardzo dobrze, bo wtedy zawsze podważamy coś, co być może jest dobre. I to sprawia, że bardziej na przykład dochodzimy do jakichś wniosków, szybciej, do ciekawszych odkryć. Tak, więc największym grzechem jest po prostu uważanie, że coś świetnie. I mamy na przykład, no kilku takich klientów, trochę jakby staramy się weryfikować tego typu podejście, że w ogóle zaczynając współpracę, klient w ogóle powiedział, akurat ja byłam na tym callu powiedział, że – u nas wszystko jest super, u nas wszystko jest świetnie. I oni powiedzieli, że oni mają wdrożone 3 rozwiązania anty phishingowe, ja mówię – dlaczego 3? – No, bo jak jeden nie zadziała, to drugi, a jak nie drugi, to trzeci. A ja mówię – a nie lepiej po prostu mieć jeden, którym będziecie zarządzać i dobrze skonfigurowany? – No nie, bo trzy to lepiej. Mówię – no dobra, no dlaczego nie macie na przykład siedem?

[00:50:00]

Paula Januszkiewicz: A oni – dlaczego siedem? Ja mówię – bo siedem to też lepiej. Więc, więc generalnie jakby często, często spotykamy się też i z takim podejściem. Ale, co ciekawe jak robiliśmy dla nich właśnie pentest, taki wewnętrzny, to się okazało, że mówimy – a no dobra, okej, zobaczymy jak w ogóle wygląda dział IT, tak. Bo dział IT właśnie twierdził, że wszystko jest super. I my wykonywaliśmy taki mega banalny, prosty atak właśnie z wykorzystaniem NetBIOS, który jest w ogóle protokołem ze średniowiecza, ale niestety domyślnie włączony w Windowsie i często wykorzystywany do ataku. No i właśnie wykorzystując NetBIOS pozwoliliśmy im się zalogować w pewne miejsce, dosłownie aż tak proste, że wstyd mi o tym mówić. I IT nie miało problemu z podawaniem swoich danych logowania właśnie w to miejsce. No, bo ja widzę, że jak zobaczyli pop-up [niepewne], taki jak na przykład się uwierzytelniasz do dysku, powiedzmy sieciowego, no to masz taki mały pop-up [niepewne]. To jest w ogóle funkcja taka w systemie client process with log in [niepewne] i tam podajesz sobie swoje dane. Tak jakby wszyscy widzieli to okno. Więc oni mieli dokładnie takie okno, no i podali tam dane logowania. Ale czemu, bo się logowali gdzie? Oni w ogóle nie rozpoznali tego kontekstu. I to było takie trochę smutne, bo jeżeli twierdzą, że są tacy świetni to, czemu podają dane do logowania na prawo i lewo. No i tak dalej, więc takich kontekstów jest cała masa.

Prowadzący: Incident Response Plan, co po włamaniu? Jak reagować, od jakich elementów zaczynać? I czy rzeczywiście organizacje mają taki Incident Response Plan?

Paula Januszkiewicz: Często nie mają niestety, często działają ad hoc. A jak mają, to coś napisane po krótce, niezweryfikowane. Więc często generalnie sam incydent tworzy absolutnie stresującą sytuację, która jest pełna chaosu. I często w takiej sytuacji dzwoni się do zewnętrznych konsultantów z prośbą o pomoc – przyjedźcie i nam to zorganizujcie tak, co musimy do tej pory zrobić. Więc, więc do tego stopnia, że, co nie uważam, że było złe organizacje podpisują na przykład chociażby z nami jakieś umowy na jakiś SLA gdzie, jeżeli oni będą zaatakowani i wykryją ten atak, to my mamy tam powiedzmy SLA i x godzin, gdzie musimy im po prostu pomóc. Więc oni podpisują taki trochę, takie trochę ubezpieczenie, bym powiedziała. I sam Incident Response Plan wymaga dobrego przygotowania i to jest podstawa dobrego planu, jak zresztą każdego innego planu. Ale taki przykład między innymi ze względu na to, że, żeby móc w ogóle zrobić zrzut pamięci, a potem zrzut dysku, to potrzebujemy jakiś storage. Potrzebujemy jakiegoś USB tak, jakiegoś dysku o określonym rozmiarze, minimum pamięć plus dysk. I nagle się okazuje, że w ogóle zdobycie takiego dysku w organizacji, kiedy trwa atak jest problemem. Co jest dla mnie absolutnie zabawna sytuacja, bo byłam w takich sytuacjach wielokrotnie, że ktoś – a, ok, mówił – to muszę mieć taki dysk, ojej, to ja takiego dysku nie mam, zamówię na Amazonie, będzie jutro.

Prowadzący: Tak i to od razu przypominają mi się akcje z jakichś różnych filmów na zasadzie woda cieknie pełnym strumieniem, a ktoś szuka jakiegoś narzędzia, aby zakręcić zawór, tak, tak.

Paula Januszkiewicz: Tak, tak, tak. Dokładnie.

Prowadzący: Słuchaj, czy biorąc pod uwagę Twoje doświadczenie w cyberbezpieczeństwie istnieje możliwość, aby działy bezpieczeństwa wskoczyły tak naprawdę w buty przestępców i dzięki temu w pewnym sensie wyprzedzały ich działania? Czy do tego są jakieś dedykowane w tym momencie szkolenia? Czy tak naprawdę właśnie kwestia monitorowania swojej sieci, patrzenia na trendy to, co się dzieje w chwili obecnej, na narzędzia, które mogą być wykorzystane, na wektory ataku?

Paula Januszkiewicz: Moim zdaniem bezpieczeństwo składa się z 3 takich podstawowych komponentów. Po pierwsze, wewnętrzna organizacja, dobre planowanie, ustalenie strategii, działanie względem niej, zgodnie z nią, ustalenie sobie jakiegoś planu właśnie, wdrożeń, tak jak mówiliśmy. Druga kwestia to jest testowanie przy wykorzystaniu firmy trzeciej. Czyli na przykład albo też posiadanie wewnętrznej jednostki do testów, która z takiego zewnętrznego, niezależnego punktu widzenia przetestuje dana infrastrukturę i bez żadnych problemów będzie w stanie nam przedstawić dokładny raport tego, co się wydarzyło wraz z rekomendacjami jak w ogóle się naprawić. Plus trzeci czynnik, to jest edukacja. I w cyberbezpieczeństwie istotne jest edukowanie się codziennie, codziennie dosłownie z tego, co to w ogóle się teraz na tym świecie dzieje. Nie mówiąc już tak o tak naprawdę o

takiej podstawowej znajomości systemów operacyjnych. I z tym jest problem, bo jedno to oczywiście wymaganie edukacji, a drugie to dostęp do informacji.

[00:55:10]

Paula Januszkiewicz: I szkoleń z cyberbezpieczeństwa jest oczywiście coraz więcej, chociażby my mamy całe Secure Academy, gdzie mamy ponad 40 szkoleń właśnie takich customowych, które uważamy, że każdy powinien, kto chce tam to przeszkolenie [niepewne] przejść, bo jakby z mojego na przykład punktu widzenia brak znajomości systemu to absolutnie, o czym my w ogóle mówimy, tak. System powinniśmy znać świetnie, bo to jest właśnie ten element, który jest zaatakowany. Więc pytanie, jak dana organizacja realizuje te, te plany, tak. Szkolenia z cyberbezpieczeństwa też nie są tanie, tak. Więc też i patrząc, bo we wszystkich w ogóle dostępnych szkoleniach z cyberbezpieczeństwa tak, są rożne certyfikacje i tak dalej. Nikt nam też nie mówi, co jest dobre, tak. Nie ma żadnego standardu. Nie ma żadnych wymogów tutaj, więc jakby często jest tak, że osoba zajmująca się cyberbezpieczeństwem musi bardzo często edukować, edukować się samodzielnie. Czyli na przykład właśnie samemu wybierać jakieś szkolenia. Jeżeli ktoś wie, czego chce, super, bo pewnie się coś tutaj znajdzie. Natomiast to często jest tak, że jak ktoś chce zacząć, to tutaj się pojawia problem, bo są tematy typu pentesty, tak, na jakichś określonych poziomach, webtesty, testy do aplikacji mobilnych. Więc często na przykład też dostajemy pytania – czy ja muszę być programistą, dobrym programistą, żeby zajmować się cyberbezpieczeństwem? Absolutnie nie, ale to się tak trochę kojarzy. No, bo ten wizerunek hakera jednak jest tą osobą, która siedzi przy komputerze i coś tam sobie klika.

Prowadzący: No klepie kod, tak, no.

Paula Januszkiewicz: Dokładnie, jakiś kod pisze, na pewno. No, więc tak też jest oczywiście, bo tym się na przykład zajmują osoby, które tworzą ransomware. Więc zależy od miejsca w infrastrukturze. I tak, jak IT jest absolutnie szeroko pojęte. Możemy się zajmować bazami danych, machine learningiem, artificial intelligence. Można pisać kod i tu też, można być testerem, quality assurance i tak dalej. Tak generalnie w cyberbezpieczeństwie jest podobnie, bezpieczeństwo sieci jest kompletnie różne od bezpieczeństwa systemów.

Prowadzący: Od bezpieczeństwa end-pointów i tak dalej. No to jest, wiadomo.

Paula Januszkiewicz: Mhm. Dokładnie. Tych, tych komponentów jest bardzo dużo.

Prowadzący: Słuchaj, nie mogę się powstrzymać, żeby nie zadać Ci jeszcze jednego pytania związanego z Twoim NVP, dobrze? Jeżeli nie masz nic przeciwko oczywiście. Jak Microsoft w chwili obecnej dba o bezpieczeństwo swoich użytkowników? Pytam z tego względu, że w jednym z poprzednich odcinków Przemek Jaroszewski wspominał pracę w CERT Polska, kiedy tak naprawdę większość jego pracy to były incydenty związane z czasami, wiesz jeszcze Windowsa XP tak, przed service packiem drugim. Wiemy,

że teraz się sytuacja mocno zmieniła. Ale jak ona w tym momencie wygląda, jeżeli chodzi o Windows 10 w odniesieniu do wcześniejszej interakcji systemu?

Paula Januszkiewicz: Absolutnie najlepiej, dlatego że mamy na przykład wbudowany w system Exploit Guard. I Exploit Guard jest tym rozwiązaniem, które właśnie wspomaga na przykład wszelkiego rodzaju techniki, powiedzmy uruchomienia kodu w pamięci procesu. Tak jakby można by tutaj wymienić całą listę tych rzeczy, które Exploit Guard ma. Natomiast generalnie jest to kolejny obszar ochrony, który ja uważam, że przez cały czas w ogóle powinien być przez ostatnie tam 20 lat, powinniśmy mieć coś takiego. Oczywiście był EMED [niepewne], był też zewnętrzny Palo Alto Traps, też właśnie Anti – Exploitation system. Więc fajnie jest, że to jest na dzień dzisiejszy wbudowane. Mamy też na przykład ochronę przed Direct Memory Access, mamy też na przykład ciekawsze podejście do Apllications Control, czyli do zapobiegania uruchamiania aplikacji, których nie znamy. Więc na dzień dzisiejszy jest, jest bardzo dobrze plus możemy w kontekście na przykład enterprisów organizacje wzbogacić w system o antywirus, czyli Protection for Endpoints, czyli Defender. I generalnie bazować właśnie na machine learningu. A Microsoft, jako jedna z niewielu, a przede wszystkim, jako jedna z pierwszych firm zajmuje się bardzo serio właśnie machine learningiem i tym intelligence threat detection, jak to się określa, czyli właśnie bazowaniem na korelacji zdarzeń. Co jest przyszłością w cyberbezpieczeństwie na pewno. Więc kiedyś było tak, że jak mówiliśmy Windows, to tak już posługuję się takim typowym stereotypem, to wszyscy – a, to niebezpieczne.

Prowadzący: [niepewne].

Paula Januszkiewicz: Tak, dokładnie. A teraz nie słyszymy tego, tak. Jakby mogą się oczywiście krzywić te osoby, które się krzywiły kiedyś, tak.

[01:00:02]

Paula Januszkiewicz: Niemniej jednak, że Windows to straszny. No i super, poczekam bardzo chętnie na argumenty. Tak naprawdę to o każdym systemie można tak powiedzieć, tak. I tutaj w żadnym wypadku nie bronię Windowsa, bo używam i Windowsa, i Linuxa, i tak dalej. Ale, ale mówię to, bo najczęściej właśnie w kierunku Windowsa się słyszało takie tego typu rzeczy. A na przykład przez ostatnie kilka lat tak naprawdę, mniej więcej od dwa tysiące, mniej więcej 2016 roku Microsoft i oni to też oficjalnie mówią, zaczął inwestować bardzo mocno w cyberbezpieczeństwo. I między innymi na przykład mamy Azure Sentinel, który pozwala nam na korelację też i zdarzeń z wielu komponentów infrastruktury, tak. Mamy też na przykład możliwość budowania maszyn wirtualnych, które na przykład wykorzystują wirtualnego TPM, tak. Czyli na przykład szyfrowanie dysku właśnie w maszynach wirtualnych w oparciu o TPM, tworzenie [niepewne], czyli maszyn, które w chmurze są generalnie zabezpieczone przed na przykład kimś, kto miałby dostęp do serwera, administrując infrastrukturą chmurową i tak dalej. Jakby poziom bezpieczeństwa wzrósł, a z punktu widzenia użytkownika

końcowego jest również, również wyższy niż to miało miejsce na przykład w systemie Windows XP, gdzie tak naprawdę każdy, nawet tam moja babcia pracowali na koncie administratora.

Prowadzący: Słuchaj, masz dostęp do kodu źródłowego Windowsa.

Paula Januszkiewicz: Tak.

Prowadzący: Czy często w swojej pracy tworząc narzędzia, korzystasz z tego przywileju? I co Ci to daje?

Paula Januszkiewicz: Czy często, to bym powiedziała, że nie. Dlatego że jest to bardzo ciekawa, niemniej jednak dosyć nużąca lektura. Więc bardzo często, kiedy mam już konkretny jakiś problem tak, co też nie zdarza się często. Jeśli mogłabym to jakoś podsumować, to może kilka razy do roku zdarza mi się skorzystać. I to też nie jest tak, że ja mam dostęp do 100%. Mam do 99%, a tak naprawdę do tego pozostałego procenta, jednego procenta ma dostęp tylko kilka osób. Więc, więc to jest tak, że nasz zespół też musi robić reverse engineering pewnych komponentów. Ja też muszę gdzieś tam rozczajać coś, ale nie ukrywam, jest to bardzo pomocne. I ja, podejrzewam zresztą jak każdy człowiek, lubię wiedzieć więcej. Bardzo frustruje mnie sytuacja, w której czegoś nie wiem. Więc, więc taki dostęp trochę łagodzi moje zapały w kontekście researchu i na pewno wspomaga efektywne wykorzystanie czasu. Więc to też jakby fajny, fajny feature, fajnie mieć, zdecydowanie fajnie mieć, ale to nie jest coś, do czego się wraca codziennie.

Prowadzący: Słuchaj, na samym początku też wspominałaś o wielu różnych narzędziach, które produkujecie w CQURE. Czy jesteś w stanie nam coś więcej na ten temat powiedzieć? Takie najciekawsze na przykład, na którymi ostatnio pracowaliście?

Paula Januszkiewicz: Mhm. Tak naprawdę to jednym z takich naszych fajniejszych setów, narzędzi mamy, tak jak już mówiłam, mamy ponad 200. I ciężko się, nawet i samemu połapać, co my tak naprawdę mamy, bo czasem jest tak, że mamy narzędzie, które jest napisane pod jakiś konkretny, pod jakiś konkretny problem. Na przykład wyciąganie [niepewne] exów, czyli plików event loga z memory dump, z pamięci systemu. W ogóle, po co ktoś miałby to robić? No, w jakimś zaawansowanym forensicu, to ma znaczenie. No, więc to jest taki konkretny przykład. Ale narzędzia, które ja bardzo lubię, to są takie dwa sety. Po pierwsze, narzędzie do Data Protection API. I to jest w ogóle nasz research, z tego, co się orientuję, to byliśmy tam pierwsi na świecie, ale nie wiem tego na pewno. I z tego, co kojarzę póki, co jedyni, którzy w pełni zrobili reverse engineering właśnie całej platformy kryptograficznej Windowsa. Więc, co się rusza my to odszyfrowujemy. Więc mamy cały zestaw narzędzi. I na przykład takim narzędziem, które ja uwielbiam jest [niepewne], czyli Data Protection API Bob Searcher. Bo dane zaszyfrowane w systemie Windows, na przykład, jeżeli sobie zapiszę hasło w przeglądarce, to też jest taki, taka forma właśnie zaszyfrowanych danych. One mają konkretne formy i schematy. I te schematy, my po prostu skanujemy cały system w poszukiwaniu tych schematów. Więc ja na przykład, właśnie robiąc forensic wiem, gdzie na przykład i jakie aplikacje były używane na tym

systemie. No to akurat może nie jest super skomplikowane, ale wiem, że te aplikacje przechowują jakieś sekrety, no i wiem, że mam jakiś cel działania. Wiem, że chce je rozszyfrować, te sekrety. Więc tu to jest taki set. A drugi set, to są narzędzia do, trochę też i forensicu, może i trochę ataku, do wyświetlania różnego rodzaju haseł.

[01:05:00]

Paula Januszkiewicz: Czyli na przykład, jeżeli mamy konto usługi i ono sobie działa, mamy usługę, która działa właśnie na jakimś tam koncie. I to konto usługi jest nie kontem wbudowanym w system, czyli nie log [niepewne] system, nie network service i tak dalej. Ale też nie group managed account, tylko takie klasyczne konto, typu [niepewne], tak. No to typ logowania, czyli log on as a service wymusza na systemie zapisanie hasła w sposób odwracany w rejestrze. No i my mamy całą masę takich narzędzi do wyciągania właśnie tego typu miss [niepewne] konfiguracji. Więc, więc jakby, jeśli czegoś potrzebujemy, to my sobie po prostu to piszemy. Bo często jest tak, że wiesz, przeglądasz Internet i zajmuje Ci więcej czasu znalezienie narzędzia i przetestowanie, a na koniec i tak ci nie daje tego, co chcesz versus napisanie tego narzędzia. Więc, jak już wiesz konkretnie, co chcesz, to często tego nie ma.

Prowadzący: A zresztą zawsze może się przydać później, prawda, jeżeli już coś macie?

Paula Januszkiewicz: Tak, tak. My już, my bardzo często wracamy do tych narzędzi. Czasami mnie zaskakuje, że mamy jakieś narzędzie i się okazało, że ono zostało wiesz, popełnione gdzieś tam po coś, a potem szukam, szukam czegoś i nagle się okazuje, że najlepsze źródło do narzędzi to jest nasze własne, jakkolwiek by to nie zabrzmiało.

Prowadzący: No, ale to jest takie miłe zaskoczenie wtedy, że już jest, już jest gotowe i można wykorzystać.

Paula Januszkiewicz: Przerażające, przerażające.

Prowadzący: Hasło dzisiejszego odcinka dla naszych słuchaczy to ….. Moim i Państwa gościem była Paula Januszkiewicz. Paula, wielkie dzięki za Twoją obecność i za rozmowę.

Paula Januszkiewicz: Również bardzo dziękuję i było mi bardzo miło, i pozdrawiam wszystkich serdecznie.

Prowadzący: Mi również. Do usłyszenia w kolejnym odcinku.