TRANSKRYPCJA – Odcinek XX

Cisco Talos Incident Response

[00:00:07]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. Mamy w naszej firmie systemy cyberbezpieczeństwa. Systemy mają swoich adminów. Mamy polityki bezpieczeństwa. Nasza firma działa, funkcjonuje, a my się cieszymy spokojem. Wieczorem, kiedy już myślimy o relaksie, odbieramy telefon i już wiemy, że z relaksu nici. Sieć, która jeszcze niedawno działała jak w zegarku albo przynajmniej tak nam się zdawało odmawia posłuszeństwa. Nasze bazy danych są szyfrowane albo, i w zależności od scenariusza są już na innym serwerze, który jest zarządzany niekoniecznie przez naszych pracowników. To tylko jeden z czarnych scenariuszy. Jak sobie poradzić? Co robić dalej? To tylko niektóre z pytań, które poruszymy dziś z moim gościem. Czym jest Incident Response? W czym może nam pomóc biorąc pod uwagę scenariusze podobne do przytoczonego przeze mnie przed chwileczką? Czy mamy przygotowane procedury na podobne przypadki? Ostry dyżur cyberbezpieczeństwa – Incident Response, czyli jak pracują brygady naprawcze? Moim dzisiejszym gościem jest Paweł Bosek – Incident Response Consultant w Cisco Talos Incident Response. Paweł, bardzo się cieszę z Twojej dzisiejszej wizyty.

Paweł Bosek: Cześć Michał. Bardzo mi miło, że mogę gościć w Twoim studiu.

Prowadzący: Paweł, tak na samym początku, jak wyglądała Twoja kariera w temacie cyberbezpieczeństwa? Dlaczego Talos i akuat ta dziedzina cyberbezpieczeństwa? Dlaczego właśnie Incident Response?

Paweł Bosek: Ogólnie moja kariera zaczęła się też w Cisco. Już dobrych kilka lat temu pracowałem w SOC, jako analityk bezpieczeństwa. Tam rozpocząłem staż, zaraz po studiach, nawet w ich trakcie. I nabierając po prostu wiedzy, czy w SOC, w Cisco, czy później w kolejnych firmach, zdecydowałem, że reakcja na zagrożenia będzie zdecydowanie ścieżką, którą ja będę podążał ze względu na różnorodność tej pracy i na ciągłą motywację do rozwoju, i ciągłe wymaganie w sumie rozwoju ze względu na to, że ataki się zmieniają praktycznie każdego dnia. Co chwilę wychodzi coś nowego i trzeba to sprawdzić, trzeba się dowiedzieć na ten temat sporej ilości rzeczy, jak to wykryć, jak to później przeanalizować i jak prawidłowo do tego podejść, i jak prawidłowo zareagować. Dlatego głównie, głównie Incident Response. Natomiast, dlaczego Talos? To pytanie w sumie jest dość, dość trudne i dość ciekawe ze względu na to, że tak, w Talosie jesteśmy konsultantami dla firm zewnętrznych. Czyli mamy klientów przypisanych do siebie, a także reagujemy ogólnie na zagrożenia, które są dość, dość globalne. Ostatnio na przykład był znany chyba wszystkim Log4j i tutaj wspieraliśmy naszych klientów przy, pzy detekcji

tego. A także, jeżeli niestety nie zdążyli odpowiednio wcześnie zareagować, wspieraliśmy ich przy analizie już powłamaniowej, co się stało, w jaki sposób ta podatność została wykorzystana i do czego atakujący mają aktualnie dostęp. Talos pozwala akurat nam przez backgroud, jaki mają Threat Intelligencowy, prowadzić swego rodzaju trackowanie grup, które atakują różne jednostki, czy to bankowe, czy to sektory energetyczne, czy, czy jakieś wielkie finanse. I pozwala to tak naprawdę już na samym początku incydentu określić, w jaki sposób możemy prowadzić tą analizę dalej, analizę dalej i w jaki sposób jak najszybciej prawidłowo zareagować u danego klienta, poprzez informację, co się działo w tego typu środowiskach wcześniej.

Prowadzący: Paweł, pytanie może niezwiązane bezpośrednio z naszym dzisiejszym tematem, ale skąd nazwa Talos? To, że mówimy rzeczywiście o mitycznym olbrzymie z brązu, czy swojego rodzaju grysów? Bo wiesz, słyszałem już dziwne opowieści, skąd na przykład wzięły się w Cisco I Speak [niepewne].

Paweł Bosek: Na to pytanie niestety nie jestem w stanie Ci odpowiedzieć. Próbowałem znaleźć tę informację, i co zespół, co menager, to trochę inna odpowiedź.

Prowadzący: Inna odpowiedź?

Paweł Bosek: W tym momencie niestety nie ma jednej spójnej u nas.

Prowadzący: Słuchaj Paweł, na samym wstępie jeszcze też myślę, że powinniśmy wytłumaczyć i rozpocząć od takiego wytłumaczenia – czym są zespoły typu Incident Response? Jakie są główne zakresy ich działania? Po co firmom takie usługi?

Paweł Bosek: Zespoły Response, są to zespoły, które odpowiadają tak naprawdę za analizę tego, co się dzieje i koordynowanie akcji różnych zespołów w celu minimalizacji zagrożenia dla firmy, i w celu minimalizacji braku kontroli biznesowej w firmie. To jest główne ich zadanie i taka jest potrzeba. A dlaczego są potrzebne dla firm? Ze względu na to, że jeżeli na przykład nastąpi jakiś wyciek danych poufnych z danej firmy, czy jest jakieś bezpośrednie zagrożenie takim wyciekiem, albo bezpośrednie zagrożenie naruszenia bezpieczeństwa w ogóle firmy w jakikolwiek sposób, czy zasad bezpieczeństwa komputera, to ten zespół jest odpowiedzialny za analizę tego, w jaki sposób to zagrożenie występuje i, w jaki sposób prawidłowo zareagować na to zagrożenie, a następnie, w jaki sposób przygotować firmę na kolejne zagrożenia, żeby nie było tutaj incydentów krytycznych ostatecznie, żeby nie była przerwana ciągłość biznesowa danej firmy.

[00:05:18]

Prowadzący: Wspominałeś już o tym wcześniej biorąc pod uwagę Cisco Talos, że, no jednak większość osób chyba, znających firmę oczywiście, kojarzy tę nazwę z Threat Intelligence. Czyli w dużym uproszczeniu, no możliwością dostępu do informacji o wskaźnikach zagrożeń, najczęściej powiedzmy niebezpiecznych adresów IP, próbek złośliwego oprogramowania, które były widziane, domen, innych

artefaktów i tak dalej, i tak dalej. W jaki sposób zespół ewoluował również do świadczenia usług typu Incident Response?

Paweł Bosek: Tak naprawdę zespół po prostu został rozbudowany ze względu na to, że część Talosa zawsze współpracowała z klientami odnośnie Threat Intelligence i odnośnie bazy danych wskaźników do tego. I część zespołu ze względu na to, że współpracowali blisko z klientami, i pomagali przy, przy analizach tego typu rzeczy, zostało zauważone, że jest potrzeba od naszych klientów większego wsparcia z naszej strony. I część zespołu threat intelligencowego została po prostu przesunięta do zespołu Incident Response, a także Forensic. I później ten zespół został, zostaje non stop rozbudowywany.

Prowadzący: A jak wygląda wewnętrzny podział zespołu, w którym pracujesz? I, czy między Wami, a właśnie częścią Threat Intelligence występuje swojego rodzaju współpraca, takie zazębianie się, czy jednak pozostają to powiedzmy, osobne zespoły?

Paweł Bosek: Jest współpraca i jest zazębianie się. Natomiast jest też jasny podział obowiązków. Incident Response Consultant odpowiada za kontakt z klientem i to wsparcie tego klienta na każdym etapie incydentów czy, czy procesu Incident Response. A analityk Threat Intelligence, czy Threat Intelligence Consultant odpowiada za wsparcie takiego Incident Response procesu od strony informacji na temat zagrożeń. Więc współpraca między nami przy każdych incydentach jest bardzo ścisła. Do każdego incydentu są przypisane odpowiednie osoby od strony Incident Response i od strony Threat Intelligence. I to te osoby odpowiadają tak naprawdę za całość akcji, analizy i detekcji, a także budowania danych na temat incydentu, co się konkretnie wydarzyło, i z jakimi grupami ma tu powiązanie, a także, jak zabezpieczyć się w przyszłości przed tego typu incydentami.

Prowadzący: Słuchaj, a kiedy najczęściej są wzywane zespoły Incident Response? Czy są to częściej przypadki takiej stałej pracy i bycia w pogotowiu? Czy dopiero jak, no tak mówiąc wprost, administratorzy załamują już niestety ręce bez mocy? Administratorzy po stronie klienta oczywiście.

Paweł Bosek: Tak, tak, tak. Tutaj sprawa wygląda, że się tak wyrażę, dwojako, ze względu na to, że jeżeli się spojrzy nawet w nasze portfolio, to są dwie usługi, reactive i cała masa, cała masa usług proactive. Czyli w większości nasi klienci, jeżeli są już dłużej naszymi klientami, jednak raczej nie współpracujemy z nimi na, na incydentach. Rzadko, kiedy się zdarza, że jeżeli firmy, które konsultują się z nami już dłuższy czas w ramach zwiększenia bezpieczeństwa swojej firmy, żeby do tych incydentów krytycznych dochodziło, że będą potrzebować naszej pomocy w minimalizacji tej straty, jaką, jaką doświadczą. Zazwyczaj jest to jednak w usługach proaktywnych, kiedy pomagamy im budować wszystkie procedury, zwiększamy ich, zwiększamy ich detekcję, zwiększamy monitoring, jaki mają w firmie, a także szkolimy ich zespoły, w jaki sposób prawidłowo to analizować, w jaki sposób

reagować. Co jakiś czas też dostarczamy im, albo usługi ofensywne w stylu red team, czy, czy purple team. Bo pentestami też się zajmujemy, natomiast bardziej oferujemy coś długotrwałego niż, niż same pentesty. Bo ogólnie nie da się zbudować polityk bezpieczeństwa raz, a dobrze, to musi non stop być sprawdzane i poprawiane dla danych środowisk. Bo każde środowisko firmowe się zmienia. Natomiast bardzo często jesteśmy wzywani przez klientów, którzy nie są jeszcze klientami Talosa. I oni potrzebują właśnie reakcji, pomocy w reakcji na, na dane zagrożenia. Zazwyczaj niestety jest to ransomware i jest to analiza już post encryption, kiedy dane zostały zaszyfrowane i tylko klienci potrzebują się dowiedzieć, jak do tego doszło i, w jaki sposób przygotować się na kolejne tego typu ataki.

Prowadzący: A co jest najważniejsze w Twojej pracy? Czy tylko przywrócenie właśnie do życia infrastruktury, czy, czy, czy tak, jak właśnie wspominałeś jak najdokładniejsze odpowiedzi na powstałe w taki naturalny sposób pytania – skąd się to u mnie wzięło, kto jest odpowiedzialny za atak, za zebranie dowodów, co dalej?

Paweł Bosek: Najważniejsza w mojej pracy jest pomoc klientowi, więc zależy, zależy od tego, co klient tak naprawdę potrzebuje.

[00:10:02]

Paweł Bosek: Są klienci, którzy potrzebują jak najszybciej reakcji, żeby się pozbyć zagrożenia z sieci, ale nie potrzebują dokładnie wiedzieć, w jaki sposób się tutaj atakujący znalazł w tej sieci ze względu na bardzo różnie zbudowane środowiska i bardzo różne polityki, a także tutaj konsekwencje prawne. Nie potrzebują wiedzieć takiej informacji, więc dla nich ta informacja jest najmniej ważna. Natomiast ważne jest dla nich, żeby się pozbyć atakującego z sieci. A także są firmy, które potrzebują dokładnie wszystko wiedzieć. I wtedy jak najbardziej kładziemy tutaj nacisk, żeby dojść do tego, jaki był wektor wejściowy i, jak atakujący uzyskiwał kolejne dostępy wewnątrz sieci.

Prowadzący: Z jakich narzędzi korzystacie w celu połączenia kropek, o ile oczywiście mogę to tak nazwać? Wiesz, o co mi chodzi. Czyli w pewnego rodzaju korelacji, analizy, złośliwego oprogramowania, czy różnego typu złośliwych kampanii.

Paweł Bosek: Z takich ogólnych narzędzi, to mogę powiedzieć, że mamy własną instancję MISP, do korelacji i do dzielenia się informacjami. Korzystamy z, do analizy próbek złośliwego oprogramowania, albo z naszych sandboxów, albo już z zespołu, który jest odpowiedzialny za reverse engineering. A do digital forensic, no to korzystamy tutaj z wszelkiego rodzaju komercyjnego i naszego oprogramowania do, do analizy czy to danych z endpointów, czy zrzutów pamięci, w zależności od tego, jaki jest incydent.

Prowadzący: Wspominałeś właśnie o forensicu i o reverse engineeringu. Dla mnie to też jest bardzo ważne, żeby tak wytłumaczyć, czym są te elementy i jaka jest ich rola w pracy zespołów Incident Response?

Paweł Bosek: To może zacznijmy od forensica. Forensic jest to na polskie tłumaczenie, o ile mi dobrze wiadomo – informatyka śledcza, czy, czy jakoś tak się to tłumaczy. Natomiast jest to po prostu z logów i z wszystkich danych dostępnych odwzorowanie i uzyskanie informacji, co dokładnie dana osoba zrobiła na danej jednostce, czy to jest Windows, czy to jest Linux, czy to jest Mac OS, czy, czy Android, czy Iphone. Odwzorowanie i uzyskanie informacji na temat wszelkich aktywności, jakie były na, na tym urządzeniu. A reverse engineering jest to po prostu wzięcie próbki danego oprogramowania i dowiedzenie się dokładnie, co ta próbka robi w danych środowiskach, i jakie są możliwości danego oprogramowania, czy to jest szkodliwe, czy nieszkodliwe. Jeżeli jest szkodliwe to, w jaki sposób, czy się komunikuje z jakimiś zewnętrznymi serwerami i jaki jest cel tego oprogramowania.

Prowadzący: Wspominałeś wcześniej na temat takiego podejścia bardziej proaktywnego. W jaki sposób przygotowuje się taki plan awaryjny, w zależności od klienta? Jak przebiega proces takiego szycia na miarę procedur związanych z Incident Response?

Paweł Bosek: Z proaktywnego podejścia pierwsze, co należy wykonać to jest Incident Response Plan. I tutaj my pomagamy klientom zbudować taki plan albo przeprowadzamy analizę ich planu i wskazujemy słabe punkty w danych planach. Natomiast ten plan powinien pokrywać tak bardzo wysokopoziomowo całe, całą gamę incydentów, głównie cyberbezpieczeństwa z naszej strony, i w jaki sposób reagować, z kim się kontaktować, jeżeli w danych grupach wystąpi incydent, żeby nie utracić ciągłości biznesowej danej fimy. I to jest usługa akurat, która jest najbardziej jakby w komunikacji z klientem ze względu na to, że potrzebujemy zrozumieć środowisko klienta, więc potrzebujemy jak najwięcej informacji odnośnie tego środowiska się dowiedzieć. Prawidłowo zbudowany Incident Response Plan zawiera informacje na temat całej infrastruktury firmy, na temat wszystkich kontaktów, jakie są wewnątrz, jakie są możliwości reagowania na różne zagrożenia w danych segmentach środowiska.

Prowadzący: Z Twojego punktu widzenia taki plan, jak szybko jest w stanie firma opracować, razem oczywiście z, na przykład z Wami?

Paweł Bosek: Jeżeli firma kładzie nacisk, żeby ten plan był dobrze skonstruowany i poświęcają tutaj czas, żeby to z nami wykonać, zazwyczaj jest to czas około miesiąca, żeby ten plan został stworzony, jeżeli firma go nie ma w ogóle, to stworzony od, praktycznie od zera. I tutaj sprawdzony przez, przez klienta też i żeby zostały naniesione poprawki, które w trakcie sprawdzenia tego planu zostały wykryte. Tak raczej minimum miesiąc jest brany pod uwagę, żeby, żeby taki plan wykonać.

Prowadzący: A czy z Twojego punktu widzenia często się zdarza, że klienci wraz ze swoimi zespołami ćwiczą takie sytuacje awaryjne, szczególnie w przypadku, no firm troszeczkę mniejszych niż tutaj o wspomnianych jakichś gigantach mówimy, zanim te rzeczywiście nastąpią?

[00:15:09]

Prowadzący: Wiesz, spotkałem się nieraz podczas rozmów z różnymi ludźmi, że, że na to troszkę narzekali, i to tak trochę, jak wdrożenie systemu backupowego, ale bez okazyjnych prób, jak zadziała w przypadku prawdziwej awarii. Niby jesteśmy przygotowani, a jednak pewnego rodzaju loteria.

Paweł Bosek: W przypadku firm troszkę mniejszych ciężko jest mi powiedzieć ze względu na to, że tutaj rzadko, kiedy współpracujemy niestety z mniejszymi firmami. Natomiast dość często współpracujemy z firmami powiązanymi ze zdrowiem, czy to są jakieś firmy, które obsługują sieci szpitali, czy, czy coś w tym stylu. I niestety bardzo często się zdarza tak, że ten Incident Response Plan mają w jakiś sposób napisany, natomiast nigdy nie został przetestowany, nigdy nie został sprawdzony. I w trakcie reagowania właśnie na tego typu incydenty wychodzą luki i błędy, jakie są w tym, w tym planie. Więc powinno się taki plan testować raz na rok, takie są best practices. Natomiast, jak to wychodzi w praktyce, bywa bardzo różnie.

Prowadzący: Paweł, jeżeli już jesteśmy przy Incident Response Planie, wydaje mi się, że jest to na tyle tak naprawdę szeroki temat, że warto byłoby tutaj troszeczkę więcej podrążyć, biorąc pod uwagę kwestie właśnie tworzenia, przygotowania, grup, z jakimi współpracujecie, aby taki Incident Response Plan przygotować. Jak to wygląda od kuchni, czyli takie poszczególne kroki, jeżeli mógłbyś nam tutaj troszeczkę więcej opowiedzieć?

Paweł Bosek: Może omówmy sobie fazy, jakie są w takim Incident Response Planie, żeby prawidłowo go ogólnie przygotować albo zweryfikować, czy jest on prawidłowo przygotowany i gotowy na wszelkie aktywności i zagrożenia. Taki plan powinien się zawierać z kilku dobrze znanych kroków. Pierwszy to jest przygotowanie. I tutaj cała kwestia jest, co się dzieje przed incydentem, przed tym, jeżeli, jak sygnatura wyskoczy nam i powie, że jest jakiś incydent, jakieś zagrożenie w naszej sieci. W przygotowaniu trzeba zrozumieć, w jaki sposób działa firma, w jaki sposób są przechowywane wszystkie logi, wszystkie danej w danej firmie. Trzeba to przetestować, czy dostęp do tych logów jest, czy da się te logi z tego miejsca przeanalizować, czy nie ma żadnego problemu z tym. Trzeba w przygotowaniu sprawdzić całe oprogramowanie firmy, czy wszystkie serwisy zewnętrzne nie są podatne, czy może są jakieś podatne. Trzeba sprawdzić procesy, w jaki sposób reagować na konkretne rzeczy, w jaki sposób się komunikować, w jaki sposób zmieniać i poprawiać infrastrukturę firmy, czy procesy w danej firmie. No i trzeba przygotować taką strategię reakcji na to zagrożenie, czy, czy na naprawę. Taki główny cel przygotowania właśnie, to jest posiadanie narzędzi i umiejętności do działania w przypadku incydentu. Następnie jest detekcja i analiza – Detection and analysis. I tutaj w zależności od tego, co zostało wykryte albo, z jakimi informacjami mamy do czynienia, z jakiego powodu uważamy, że jest to incydent krytyczny. W tej fazie, w Incident Response Planie powinno, powinien być zaplanowany monitoring, który nada nam priorytet na konkretne rzeczy, będziemy

wiedzieli, z jakimi metodami ataku możemy się spotkać, jakie są nasze krytyczne systemy, które musimy, na które musimy jak najbardziej zwracać uwagę. Następnie, w tej detekcji i analizie powinniśmy mieć opisany proces segregacji i eskalacji tych alertów i eventów, które mamy, żeby było wiadome, które wyeskalować do danego incydentu i, które powinny zostać przeanalizowane przez, przez grupę specjalistów. Powinniśmy mieć tutaj też informację, jak zaklasyfikować dany incydent i, z czym dana klasyfikacja się wiąże. Wiemy, że mamy tutaj RODO i GDPR, które bardzo mocno nas obligują do informacji klientów, czy w Europie, czy w Ameryce o wszelkich zagrożeniach. I bardzo tutaj ta klasyfikacja incydentu wymaga tą informację RODO, czy GDPR. Jeżeli jakiekolwiek informacje odnośnie danych prywatnych zostały udostępnione atakującym, ta informacja powinna się pojawić. W detekcji i w analizie najważniejsze jest zapis wszystkich logów, które są powiązane z incydentem, czy to są logi sieciowe, czy to są logi z jednostki końcowej, czy to są zdarzenia systemowe, czy jakiekolwiek inne logi. Jeżeli uzyskujemy informację, że na przykład dany komputer został w pełni zaatakowany i atakujący ma jakiś dostęp do niego ciągły, to możemy zrobić zrzut pamięci RAM i zrzut dysku danej jednostki, w celu późniejszej analizy albo równoczesnej analizy, żeby uzyskać jak najwięcej wskaźników informacji na temat danego zagrożenia.

[00:20:20]

Paweł Bosek: W momencie, kiedy już wszystko przeanalizowaliśmy, wiemy, jaki jest zakres danego incydentu, to wchodzimy w fazę powstrzymania. W fazie powstrzymania bardzo ważna jest wiedza na temat zasobów i zrozumienie tych zasobów, jaką funkcję pełnią, i znowu tutaj, jaka jest krytyczność tych systemów, i opracowanie metody powstrzymania tego zagrożenia dla tych systemów. Co jest ważne, tych metod powinna być więcej niż jedna. Często zdarzało się tak, że klienci mieli opracowaną jedną metodę do powstrzymywania w całej firmie, a okazywało się, że niestety ta metoda nie działała w danym przypadku i w danych incydentach, bo zmienili na przykład przez covida podejście firmowe, mają część pracy spoza biura i bez vpna, i do takich urządzeń dostępu nie mają. Więc powinna ta metoda być przetestowana wcześniej i sprawdzona, i powinna być możliwa reakcja. No i jak już będzie to tak sprawdzone i możliwe, to powinniśmy pomyśleć nad automatyzacją, w zależności od, od danych rozwiązań w firmie, w jaki sposób zautomatyzować i reagować na incydenty i powstrzymywać różne, różne zagrożenia. Po wstrzymaniu warto by też było dodatkowo jeszcze nakreślić informację, w jaki sposób robić employment [niepewne], niestety nie znam polskiego odpowiednika, różnego rodzaju oprogramowania, które pomoże nam w reakcji na dane zagrożenie. Także powinna być stworzona polityka albo procedura resetu haseł w całej, w całej firmie, w całym przedsiębiorstwie ze względu na to, że często się zdarza, że atakujący ostatecznie uzyskują dostęp do tej, do tej bazy danych na Active

Directory i powinna być możliwość, przetestowana możliwość resetu haseł w zależności od zapotrzebowania, i żeby to nie było tworzone w trakcie, w trakcie incydentu.

Prowadzący: W biegu po prostu nie [niesłyszalne].

Paweł Bosek: Dokładnie. Dokładnie. Następnie już kończąc aktywności incydentowe stricte, czyli usunięcia atakującego z wewnątrz sieci i odtworzenie ciągłości biznesowej. Tutaj bardzo warte uwagi są wszelkie backupy i ustalenie progu ryzyka, kiedy uważamy, że system jest czysty, a kiedy stwierdzamy, że trzeba go całkowicie odbudować, i przywracać ciągłość firmy z tych backupów oraz odzyskanych systemów. No i przechodzimy do aktywności po incydencie, czyli tak zwane lessons learned oraz rekomendacje. To się dzieli na, na dwa tak naprawdę etapy ze względu na to, że lessons learned są stricte do Incident Response procesu, do tego procesu reakcji na zagrożenia, i w tym powinniśmy przejść przez ten cały proces reakcji na dany incydent krytyczny, wskazać wszelkie problemy, z którymi się zmierzyliśmy, wszelkie słabości, jakieś punkty poprawy. I napisać to w Incident Response Planie, poprawić po prostu ten, ten plan reakcji. A także rekomendacje tutaj do, do systemów, czyli już na przykład zmiana części infrastruktury firmy, wprowadzenie segmentacji, wprowadzenie wieloskładnikowego uwierzytelnienia, czy coś w tym stylu. Powinniśmy stworzyć projekty, w których będziemy śledzić te rekomendacje, żeby one zostały faktycznie wdrożone w firmie i, żeby poprawiały bezpieczeństwo naszej firmy.

Prowadzący: I jak wyglądają takie testy?

Paweł Bosek: Są to na przykład typowe scenariusze do, do table topów [niepewne], gdzie zakłada się, że firma została zaszyfrowana w jakiś sposób i przechodzi się po prostu przez cały Incident Response Plan, w jaki sposób zareagować, i czy ta reakcja byłaby poprawna, czy ta reakcja wymagałaby jednak jakiegoś dalszego rozwoju, dalszej współpracy, żeby prawidłowo zareagować w danym środowisku.

Prowadzący: Widzicie i analizujecie różne kampanie. Jak najczęściej rodzą się te wielkie? Jak aktorzy [niepewne] próbują pozostać w ukryciu przygotowując infrastrukturę pod atak? Wiesz, praca, która wymaga czasami masę czasu i może pozostawiać wiele śladów, a jednak czasami wybucha nam przed nosem całkowicie niespodziewany. Czyli z jednej strony monitorowanie, ale również takie przewidywanie ruchów napastnika.

Paweł Bosek: To myślę, że najlepszym przykładem będzie aktualnie grupa Conti, gdzie byli oni pierwsi, którzy, gdy wyszła podatność Log4j wykorzystali to po zaledwie kilku dniach i zaczęli zdobywać dostępy do środowisk swoich ofiar, a następnie szyfrowali te środowiska.

[00:25:10]

Paweł Bosek: Więc wszelkie wskaźniki, jeżeli będziemy monitorować pod względem ich aktywności na bazie różnych incydentów, a także na bazie dostępnych źródeł, to będzie to jak najbardziej przydatne w monitorowaniu takich wielkich grup czy kampanii.

Prowadzący: Słuchaj, wspominałeś, że bardzo często spotykasz się oczywiście z ransomwarem i to jest wydaje mi się, że też sprawa, sprawa jasna, a z jakimi jeszcze innymi przypadkami najczęściej macie do czynienia? Co pojawia się tak powiedzmy w pierwszej trójce, jeżeli mogę o to zapytać?

Paweł Bosek: A pytamy już o taki wynik końcowy, czy pytamy o całość, na przykład top trendów, jakie, jakie istnieją?

Prowadzący: Top trendów, z jakimi Ty, jako właśnie pracownik Talosa się spotykasz u swoich klientów i jesteście wzywani?

Paweł Bosek: To z top trendów ransomware będzie, jako, jako pierwszy ze względu na to, że to jest 40% naszych, naszych incydentów. Tak mniej więcej w ciągu ostatniego roku. Główne kolejne trendy to jest jednak problem z emailem. Bardzo dużo kampanii phishingowych obserwujemy. Jest to bardzo wzmocnione i bardzo wykorzystywane przez atakujących, więc security awareness training dla, dla wszystkich, kto tylko ma dostęp do maila, byłoby super. Natomiast główna podatność, jaka jest, a raczej główny problem, jaki jest też wśród firm, to brak wieloskładnikowego uwierzytelnienia. Często się zdarza tak, że na przykład, żeby się zalogować do maila lokalnie potrzeba kodu na przykład z telefonu, czy, czy cokolwiek, z jakiejś aplikacji. Natomiast, jeżeli się logujemy już bezpośrednio na stronie [niesłyszalne], to tego kodu już nie potrzebujemy. Więc to, to wieloskładnikowe uwierzytelnienie powinno być wszędzie, bo daje możliwość atakującemu tak czy siak dostęp do jakichś zasobów wewnętrznych, jeżeli go nie ma, a te zasoby wewnętrzne jak najbardziej powinny być chronione.

Prowadzący: Wspominałeś o phishingu, o mailach, ale w, o jakiej formie tak naprawdę phishingu tutaj też najczęściej mówimy? Czy chodzi nam tutaj bardziej o kwestie kompromitacji poświadczeń i dobrania się powiedzmy do, do skrzynki pocztowej, czy, czy scenariusze wyglądają często inaczej?

Paweł Bosek: Scenariusze wyglądają bardzo różnie. I to zależy już od inwencji twórczej i od celu atakującego. Ze względu na to, że bardzo dużo jest maili phishingowych, które są z jakimś linkiem czy załącznikiem, żeby uzyskać dostęp do, do maszyny bądź do konta. Ale też się spotykamy z phishingiem w stylu, że jest już dostęp do jakiegoś konta, jest rozsyłany phishing wewnątrz firmy dalej w celu defraudacji pieniędzy, w celu wykonywania przelewów czy, czy tego typu rzeczy. Spotkaliśmy się też nieraz z phishingiem, który wyłudzał informacje na temat jakichś aktualnych aktywności firmy, a następnie te, te informacje zostały publikowane w dark webie i na bazie tego był szantaż, że kolejne informacje będą publikowane, i klient musi zapłacić okup, żeby nie zostało to opublikowane. Więc tutaj z phishingiem praktycznie wszystkie chyba możliwe scenariusze są jak najbardziej widoczne i aktywne.

Prowadzący: Kilkukrotnie wspominałeś o głośnej sprawie Log4j, natomiast, jeżeli możesz się z nami podzielić, jeszcze jakieś inne najciekawsze casy, nad którymi ostatnio pracowaliście?

Paweł Bosek: Najciekawsze z mojego punktu widzenia to będą jednak casy ransomwarowe albo analizy insiderowe, ze względu na to, że insider threat jest jednym z najtrudniejszych casów, bo, bo trzeba tam dokładnie przeanalizować, co dany użytkownik zrobił. Natomiast jest to też bardzo ciężkie, bo zazwyczaj nie ma tutaj żadnych sygnatur, czy, czy rólek detekcyjnych [niepewne], które wsparłyby naszą analizę. To trzeba po prostu przeanalizować wszystkie systemy pod względem danego użytkownika, wszystkie dostępne systemy. Natomiast bardzo często się pojawia, pojawia ransomware i tutaj w zależności od tego, co jest aktualnie znane i niezałatane, na przykład tak, jak teraz były akcje z Log4j, tak wcześniej były z exchangem [niepewne]. Bardzo dużo tego jest po prostu i bardzo dużo tego analizujemy i pomagamy klientom w reakcji na zagrożenia, a także informacje, w jaki sposób, jak już dojdzie do złamania danej podatności, do wykorzystania przepraszam danej podatności, w jaki sposób mogą wykonać detekcję później, żeby jednak nie doszło do tego celu finalnego zaszyfrowania całej firmy i wszystkich danych.

Prowadzący: A jeżeli już mówimy tutaj o sytuacjach związanych z ransomwarem, i jeżeli jesteście wzywani, gdzie te dane już zostały zaszyfrowane, jak często zdarza się Wam pomóc klientowi, oprócz oczywiście tak, jak wspominałeś forensic, oprócz zebrania pewnych informacji, aby, no tak naprawdę przywrócić pliki do pierwotnej postaci? Czy to przez właśnie odzyskanie w taki, czy inny sposób od napastnika klucza, czy wykorzystanie dekryptora?

[00:30:12]

Paweł Bosek: Jeżeli tylko mamy możliwość odszyfrować te dane, jeżeli znamy programy, które zostały wykorzystane, te próbki programów, które zostały wykorzystane do zaszyfrowania danych i wiemy, że są tam jakieś podatności, to staramy się odzyskać te dane dla klientów. Natomiast bardzo często jest to niestety niemożliwe aktualnie. Trzeba albo negocjować z atakującym, co też jest bardzo tutaj ciężkie ze względu na to, że na przykład w Ameryce jest teraz prawo, że nie można płacić okupu, ale jak wiemy po statystykach na przykład kont i ten okup bardzo dużo im firm płaci. Więc staramy się odzyskać te dane, ale nie zawsze jest to niestety możliwe.

Prowadzący: Czy czasami też uczestniczycie w takich rozmowach z napastnikami, jeżeli chodzi tutaj o kwestie odszyfrowania?

Paweł Bosek: Ja nie uczestniczę w takich rozmowach i z tego, co wiem, żaden z moich kolegów też nie.

Prowadzący: Paweł słuchaj, poważna sprawa dotycząca Polski, bo to już też poruszałem kilkukrotnie, ale nie mógłbym sobie odmówić, aby, aby Ciebie nie zapytać. Polska, jako cel cyberprzestępców – czy

pracujecie również na naszym podwórku bądź macie kontakt z aktorami, którzy występują na naszej, no u nas tak naprawdę w kraju?

Paweł Bosek: Wspieramy polskich klientów, pracujemy tutaj, a także mamy rozpisane kampanie, które się przeciwko Polsce działy, mamy rozpisane wskaźniki grup, które wiemy, że, że atakują Polskę. I monitorujemy też te trendy, jak się zmieniają pod względem ruchu do i z Polski.

Prowadzący: Moim i Państwa gościem był Paweł Bosek z Cisco Talos. Paweł, jeszcze raz, bardzo dziękuję Ci za Twoją obecność i rozmowę.

Paweł Bosek: Bardzo Ci dziękuję Michał.

Prowadzący: Do usłyszenia w kolejnym odcinku.

Paweł Bosek: Do usłyszenia.