

Dzień Dobry,

Nazywam się Dariusz Jeznach. Reprezentuję Wydział Naruszeń w Departamencie Kontroli i Naruszeń Urzędu Ochrony Danych Osobowych.

Witam Państwa na drugim z kolei webinarium. Poprzednie odbyło się w czerwcu 2021 r. i poświęcone było zgłaszaniu w praktyce naruszeń ochrony danych osobowych organowi nadzorcemu, w tym zgłaszanie naruszeń informatycznych. W tym wystąpieniu postaramy się wspólnie z przedstawicielem Wydziału Kontroli i Naruszeń panem Tomaszem Ochmińskim odpowiedzieć na zadane nam pytania dotyczące zabezpieczeń systemów informatycznych. W drugiej części Tomasz przedstawi aspekty techniczne, jakie administrator może zastosować podczas przetwarzania danych osobowych. Wśród poruszanych zagadnień będzie wprowadzenie do zarządzania podatnościami. Cykl zarządzania tego typu podatnościami w środowisku informatycznym jest jednym z kluczowych elementów dobrze funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji i wymaga wdrożenia odpowiednich narzędzi.

Ja natomiast postaram się Państwu przybliżyć aspekty prawne oraz odpowiedzieć na pytania związane z prawnym podejściem do tego zagadnienia.

Jednakże na początku chciałbym podkreślić, że Urząd Ochrony Danych Osobowych nie reklamuje oraz nie poleca produktów oferowanych przez poszczególnych krajowych i międzynarodowych vendorów, dostawców oprogramowania dedykowanego dla poszczególnych odbiorców, oferowanych usług informatycznych, dostawców usług hostingowych, dostawców platform internetowych. Organ nadzorczy wskazuje jedynie na możliwość stosowania pewnych rozwiązań, mogących mieć wpływ na podwyższenie poziomu bezpieczeństwa przetwarzanych danych osobowych. Nie prowadzi również certyfikacji stosowanych rozwiązań informatycznych ani stosowanego przez administratorów sprzętu oraz urządzeń jak również oprogramowania hardwareowego i softwareowego. Odradzałbym ponadto stosowanie oprogramowania nielegalnego, nielicencjowanego, pochodzącego z nieznanych źródeł, pozbawionego wsparcia producenta. Dotyczy to oprogramowania w którym przetwarzane są dane osobowe, jak również komputerów, serwerów, kart pamięci czy telefonów komórkowych. O ile w przypadku komputerów głównie stosowane jest oprogramowanie Windows i Linux, w przypadku telefonów komórkowych tym oprogramowaniem jest w przeważającej części Android. Ma to szczególne znaczenie po wystąpieniu incydentu technicznego, kiedy administrator musi wykazać, że właściwie stosował się do przepisów tj.: zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu przetwarzania, minimalizacji danych, prawidłowości, ograniczenia przetwarzania, integralności, poufności. W myśl tych zasad administrator, współadministrator lub podmiot przetwarzający będą musieli przed organem nadzorczym wykazać, że wdrożyły te zasady i stosują je prawidłowo.

Nie padną tutaj żadne nowe twierdzenia ani nie zostanie powiedziane to co powszechnie jest już znane czyli, to że organ nadzorczy w swoich decyzjach opiera się art. 24, 25, 32 rozporządzenia 2016/679 oraz wyrokach Wojewódzkiego Sądu Administracyjnego w Warszawie, który w swoich uzasadnieniach po pierwsze stwierdza np.: że: Wyroku z dnia 3

września 2020 r., sygn. II SA/Wa 2559/19, „Rozporządzenie 2016/679 wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu. Podmioty przetwarzające dane osobowe zobligowane są nie tylko do zapewnienia zgodności z wytycznymi ww. rozporządzenia poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka.

Po drugie: wyrok Wojewódzkiego Sądu Administracyjnego z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19 „czynności o charakterze techniczno-organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka oraz charakteru chronionych danych osobowych.”

Niewskazywanie wprost administratorom warunków brzegowych stosowanych środków bezpieczeństwa przez organ nadzorczy nie wynika ze złych intencji, jak również nieprzyjaznego nastawienia Urzędu Ochrony Danych Osobowych w stosunku do podmiotów danych. Takie środki nie zostały dotychczas wskazane w rozporządzeniu 2016/679. Rozporządzenie nałożyło na administratorów, współadministratorów oraz podmioty przetwarzające stosowanie odpowiednich środków, a na organ nadzorczy ich każdorazowe indywidualne sprawdzanie.

Na korzyść indywidualnego doboru środków technicznych i organizacyjnych przez administratorów przemawia konieczność stosowania różnych środków dla poszczególnych zdarzeń i incydentów technicznych skutkujących naruszeniem ochrony danych osobowych. I tak nieporównywalne są zdarzenia zagubienia, utraty lub kradzieży komputerów lub urządzeń pamięci przenośnej, gdzie należy urządzenia te zabezpieczyć przed nieautoryzowanym dostępem, ze zdarzeniem zaszyfrowania serwerów oprogramowaniem ransomware gdzie istnieje konieczność wykonania niewspółmiernie większej pracy. Oczywiście oba te zdarzenia należy uwzględnić w analizie ryzyka, właściwie je oszacować i zmitigować. W przypadku kradzieży komputera mitygowanie ryzyka nastąpi poprzez np.: zastosowanie loginu i hasła oraz szyfrowania dysków twardych komputera, co na chwilę obecną uniemożliwi ujawnienie danych osobowych w przypadku ich utraty. W drugim przypadku jest to wykonanie analizy ryzyka całego systemu, co jest procesem dużo bardziej czasochłonnym, skomplikowanym i zaawansowanym. Właściwe oszacowanie ryzyka polega m. in. na podzieleniu na to, które wyniknęło z błędu ludzkiego czyli np.: phishing (w tym celu stosujemy zabezpieczenia organizacyjne w postaci szkoleń, treningów, testów) oraz techniczne zabezpieczenia:

zabezpieczanie otwartych portów, firewalla, antywirusy, segmentację sieci, autoryzacja poprzez sms, unikanie nazw użytkownika i haseł typu: admin, admin, qwerty, 123456).

W decyzjach wydawanych przez Prezesa Urzędu Ochrony Danych Osobowych w latach 2019 - 2022 organ nadzorczy w pierwszej kolejności brał pod uwagę, czy doszło do utraty poufności, integralności i dostępności, następnie, czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W dalszej kolejności sprawdzał poprawność wykonanej analizy ryzyka, następnie czy administrator wywiązywał się w sposób prawidłowy z nałożonych na niego obowiązków dotyczących wdrożenia odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającego temu ryzyku, w tym zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Organ nadzorczy dokonując oceny korzystał również z uprawnień naprawczych przewidzianych w art. 58 ust 2 rozporządzenia 2016/679.

W przypadku decyzji upominawczych organ nadzorczy dotychczas brał pod uwagę takie okoliczności jak:

- a. utrata dostępności do danych osobowych,
- b. czas po którym dane osobowe zostały odtworzone z kopii zapasowych,
- c. wystąpienie wysokiego ryzyka naruszenia praw lub wolności osób fizycznych,
- d. stosowanie przez administratorów aktualnego oprogramowania,
- e. stosowanie przez administratorów odpowiednich procedur odtworzenia danych osobowych z kopii zapasowych po wystąpieniu incydentu technicznego, w tym przechowywania kopii na różnych nośnikach,
- f. stosowanie przez administratorów stałego monitorowania i aktualizacji systemów służących do przetwarzania danych osobowych.
- g. brak właściwie sporządzonych analiz ryzyka.

Dotychczas wydane decyzje miały na celu poprawienie przez administratorów stwierdzonych uchybień w postaci:

- a. długotrwałego odtwarzania danych osobowych po wystąpieniu incydentu technicznego.
- b. poprawienia lub/i aktualizacji procedur odtwarzania danych osobowych po naruszeniu.
- c. ponowne sporządzanie analizy ryzyka w celu uwzględnienia zagrożeń w postaci ataku złośliwym oprogramowaniem ransomware lub phishingu wraz ze sposobami zarządzania ryzykiem oraz jego mitygacji.
- d. Używanie przez administratorów aktualnego oprogramowania w przetwarzaniu danych osobowych.

Wybrane zagadnienia techniczne:

1. Używanie aktualnego oprogramowania w tym używanie oprogramowania wspieranego przez producenta.

2. Uzupełnienie analizy ryzyka o brakujące elementy.

Zaktualizowanie analizy ryzyka poprzez dodanie zagrożeń związanych z atakiem za pomocą złośliwego oprogramowania typu ransomware, zastosowania phishingu, spear phishingu oraz sposobów ich mitygacji poprzez wprowadzenie skutecznych technicznych i organizacyjnych metod ich eliminacji np.: szkolenia personelu w zakresie nieotwierania programów, linków pochodzących od nieznanego nadawcy, stosowanie zabezpieczeń technicznych tj.: ochrona poczty, kopie bezpieczeństwa, stosowanie programów antywirusowych bazujących nie tylko na sygnaturach wirusów ale również na analizie zachowania i wykrywaniu anomalii np.: FIM (File Integrity Monitoring), ochrona DNS polegająca na blokowaniu znanych domen wykorzystywanych przez cyberprzestępców, zarządzanie dostępem do danych, zarządzanie podatnościami czyli używanie zawsze zaktualizowanego oprogramowania, aktualnych „łatek”, zarządzanie aplikacjami, czyli dopuszczanie do użytku jedynie sprawdzonych i zaufanych aplikacji.

3. Kopie zapasowe systemu.

W przeważającej liczbie prowadzonych postępowań administrator nie dokonywał regularnego testowania, mierzenia oraz oceniania wykonanych kopii zapasowych co w rezultacie prowadziło do braku możliwości odtworzenia danych osobowych po incydencie technicznym. Nierzadko istniała konieczność odtwarzania danych z wersji papierowej. Powyższe spowodowane było brakiem odpowiedniej procedury wykonywania kopii zapasowych, a w następstwie zapisywania ich na tym samym nośniku w tej samej lokalizacji. Powodowało to niejednokrotnie sytuacje w której kopie zapasowe podczas ataku ransomware były szyfrowane razem z zaatakowanymi zasobami.

W celu uniknięcia tego typu skutków można stosować zasadę posiadania trzech egzemplarzy danych. Kopie danych należy przechowywać w co najmniej dwóch różnych typach pamięci masowej, na przykład na wewnętrznym dysku twardym i nośniku wymiennym (taśmie, serwerze, zewnętrznym dysku twardym, dysku USB, karcie SD, płycie CD lub DVD, a nawet co się jeszcze zdarza dyskietce) lub na dwóch wewnętrznych dyskach twardych znajdujących się w różnych lokalizacjach. Ważne jest fizyczne odseparowanie kopii danych.

Na czym dokładnie polega przestrzeganie reguły 3-2-1 w odniesieniu do kopii zapasowych:

- Posiadanie co najmniej trzech egzemplarzy danych. Zadania backupu można skonfigurować tak, aby tworzyć kilka kopii zapasowych każdej maszyny wirtualnej VMware lub Hyper-V.
- Przechowywanie egzemplarzy na dwóch różnych nośnikach. Rozwiązanie to obsługuje różne rodzaje pamięci masowej: taśmy, dyski, chmurę i nie tylko. Kopie zapasowe można przechowywać na dowolnym nośniku.

- Przechowywanie jednej kopii zapasowej na zewnątrz firmy. Konfigurując zadania powielania kopii zapasowych, można spowodować szybsze transferowanie kopii do lokalizacji zewnętrznej za pomocą wbudowanej akceleracji sieci WAN lub przesyłać kopie zapasowe do zewnętrznego repozytorium udostępnianego przez usługodawcę.

Decyzje o nałożeniu administracyjnych kar pieniężnych dotyczą głównie utraty poufności danych osobowych przez administratora.

Jeżeli weźmiecie Państwo pod uwagę wszystkie wskazane przeze mnie w wystąpieniu okoliczności w dość łatwy sposób wyciągniecie wnioski jakie ustalenia organu nadzorczego są brane pod uwagę przy wydawaniu decyzji o nałożeniu kar administracyjnych.

A teraz przejdę do odpowiedzi na zadane przez Państwa pytania,

1. Czy oprócz odnotowania faktu wykonania testu przywracania kopii zapasowej danych osobowych, niezbędny jest dowód zawierający wynik tego działania?

Tak, potrzebny jest pisemny dowód. Powinien być wiarygodny i zgodny ze stanem faktycznym, zgodnie z zasadą rozliczalności, która nakłada na administratora danych ciężar dowodowy, polegający na konieczności wykazania przez niego przed organem nadzorczym dowodów na przestrzeganie wszystkich zasad przetwarzania danych.

2. Czy UODO autoryzuje krajową jednostkę certyfikującą takie systemy IT i aplikacje zapewniające niezbędny poziom ochrony przetwarzanych danych osobowych? co ew. użytkownikom takich systemów daje gwarancję bezpieczeństwa i ochrony zasad przetwarzania danych osobowych zgodnie z RODO.

Odpowiedź znajduje się na stronie internetowej UODO i wskazuje, że:

Nie jest jeszcze możliwe uzyskanie od Prezesa Urzędu Ochrony Danych Osobowych czy innego podmiotu certyfikatu zgodności działania z RODO oraz wskazanie zatwierdzonych jednostek certyfikujących.

W związku z powyższym:

- Do dnia dzisiejszego żadne firmy nie wystąpiły o certyfikat ani nie otrzymały go od UODO. Nie jest także wyznaczony koszt uzyskania certyfikatu.
- Nie została sporządzona żadna lista dokumentów wymaganych, by administrator danych otrzymał certyfikat lub inny podmiot nabył uprawnienia do nadawania certyfikatów.
- Prezes UODO nie prowadzi prac nad stworzeniem krajowych kryteriów akredytacji oraz certyfikacji, o których mowa odpowiednio w art. 13 i 16 ustawy o ochronie danych osobowych. Nie jest w związku z tym znana data udostępnienia ww. kryteriów na stronie BIP Prezesa UODO.

3. Co jeśli usunięcie wykrytej podatności jest kosztowne i wymaga wysokich kosztów dla biznesu, dotyczy wąskiego zakresu danych, jednak została zidentyfikowana w kluczowym systemie dla administratora? Jaka jest rekomendacja postępowania?

Odpowiadając na to pytanie, trzeba stwierdzić jak z przyjętą formułą "to zależy":

Czy zakres danych w przypadku ich naruszenia spowoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli występuje wysokie ryzyko związane z wystąpieniem incydentu technicznego dotyczącego tej podatności i to ryzyko nie będzie w żaden sposób mitygowane to te dane osobowe nie powinny być przetwarzane przez administratora. Musi on zastosować adekwatne środki w celu zminimalizowania wystąpienia ww. zdarzenia. Może również z uwagi na wysokie koszty zmitigować to ryzyko poprzez przekazanie danych np. podmiotowi dysponującemu odpowiednimi narzędziami w celu obniżenia ryzyka. W tym celu administrator może podpisać z takim podmiotem umowę powierzenia zgodnie z art. 28 RODO. Administrator samodzielnie podejmuje taką decyzję.

4. Czy wdrożenie przez procesora ISO 27001 daje administratorowi wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą? Mając na uwadze, że stosowanie zabezpieczeń powinno być traktowane jako ciągły proces, a nie jednorazowe wdrożenie, to pytanie czy UODO rozważa wprowadzenie jako obowiązkowe lub rekomendowane dla podmiotów stosowanie wytycznych norm ISO 27000 oraz ISO 22301?

ISO 27001 to uznawana na całym świecie norma obejmująca systemy zarządzania bezpieczeństwem informacji. Ma za zadanie pomóc organizacjom przestrzegać najlepszych praktyk, aby ich informacje pozostały bezpieczne. Wskazać należy na słowo „pomóc”. Jak wskazano w pytaniu ochrona danych osobowych to proces nie jednokrotne działanie, także wdrożenie tych norm może być dobrze postrzegane przez organy nadzorcze i inne organizacje, jednak samo ich wdrożenie nie daje wystarczających gwarancji przestrzegania tych norm. Można sobie wyobrazić sytuację w której normy te praktycznie nie są przestrzegane w organizacji mimo ich wdrożenia. Konieczne jest stosowanie dodatkowych działań audytowych i kontrolnych. Odpowiadając na drugą część pytania, w chwili obecnej nie istnieje obowiązek stosowania ww. norm przez administratorów oraz inne podmioty.

5. Czy UODO dysponuje wykazem/listą certyfikowanych aplikacji oraz systemów zabezpieczenia i ochrony przetwarzanych danych osobowych?

Na chwilę obecną Organ Nadzorczy nie dysponuje taką listą.

6. Co należy zrobić z dyskami przeznaczonymi do likwidacji, które mogą zawierać/zawierają dane osobowe? Jakie minimalne działania będą wystarczające?

Dyski należy fizycznie zniszczyć w taki sposób aby uniemożliwić osobom nieuprawnionym odtworzenie danych na nich się znajdujących.

7. Czy podczas wrześniowego webinaru będzie poruszany temat sygnalistów?

Na życzenie osoby pytającej odpowiadam. Dnia 7 lipca 2022 r. na stronie Rządowego Centrum Legislacji opublikowano trzeci projekt ustawy o ochronie osób zgłaszających naruszenia prawa (tzw. sygnalistów) z dnia 4 lipca 2022 r wraz z uzasadnieniem. Utrzymany został charakter i nadrzędny cel nowych regulacji tj. ochrona przed odwetem sygnalistów tj. osób fizycznych zgłaszających prawdziwe informacje o naruszeniach prawa, uzyskanych w kontekście związanym z pracą. Zgodnie z informacjami dostępnymi na stronie Rządowego Centrum Legislacji, projekt jest na etapie opiniowania. Zanim trafi on do łaski marszałkowskiej będzie wymagał ostatecznego zatwierdzenia przez Radę Ministrów.

Reasumując moje wystąpienie: organ nadzorczy oczekuje od administratorów, że analiza ryzyka powinna być wykonywana przed i po incydencie technicznym naruszenia ochrony danych osobowych, powinny być wpisywane w zgłoszenie środki stosowane przed i po incydencie oraz wszystko co dotyczy kopii zapasowych (w jaki sposób są wykonywane, jak szybko odtworzono dane osobowe i dlaczego tak długo).

Na koniec mojego wystąpienia, zanim przekaze głos Tomaszowi Ochmińskiemu, chciałem Państwu serdecznie podziękować za zadane pytania. Mam nadzieję, że choć w niewielkim stopniu przybliżyłem Państwu tematykę ochrony danych osobowych i odpowiedziałem w sposób wyczerpujący na nurtujące Państwa pytania. Wychodząc naprzeciw Państwa oczekiwaniom starałem się cytować jak najmniej przepisów rozporządzenia 2016/679, a w zamian za to przekazać jak najwięcej wskazówek praktycznych oraz wskazać, jakie przesłanki są brane pod uwagę przez organ nadzorczy po wystąpieniu incydentów technicznych naruszeń ochrony danych osobowych.

Do zobaczenia na kolejnym webinarze.

Teraz przekazuje już głos Tomaszowi Ochmińskiemu w celu przybliżenia Państwu ściśle technicznych aspektów zabezpieczenia danych osobowych.

Dzień dobry Państwu. Nazywam się Tomasz Ochmiński. Dzisiaj przedstawię zagadnienia związane z zabezpieczeniami technicznymi przetwarzanych danych osobowych na podstawie przesłanych przez Państwa zapytań, za które serdecznie dziękuję. Ja tu w swojej części skupię się głównie na pytania stricte dotyczących zagadnień technicznych. Część Państwa pytań dotyczyła ogólnie zabezpieczeń i tu małe przypomnienie. Zagadnienia dotyczące tych tematów

zostały przedstawione na poprzednim moim wystąpieniu do obejrzenia, którego gorąco Państwa zachęcam.

Ten slajd pochodzi właśnie z tamtego wystąpienia, a link do tego wydarzenia zamieszczam poniżej. Jednakże w celu dokładniejszego doprecyzowania poszczególnych tematów, które zostały poruszone w Państwa zapytaniach, niektóre z tych punktów zostaną rozwinięte w tej prezentacji. I tak na początku omówimy sobie zagadnienia związane z monitorowaniem sieci.

Przede wszystkim musimy mieć świadomość, że w naszych sieciach lokalnych przepływa mnóstwo pakietów danych różnego typu. W momencie, kiedy nie monitorujemy przepływu tych pakietów, nie mamy świadomości, jakie działania w tej sieci zostają wykonane, chociażby skanowanie adresów sieciowych dokonane przez osobę postronną, co może stanowić dopiero wstęp do przygotowywanego ataku. A wystarczy uruchomić dowolny analizator protokołów sieciowych, żeby zobaczyć, co dzieje się w sieci na tym poziomie. Dlatego musimy mieć świadomość, że wśród tych danych znajdują się również nasze dane uwierzytelniające, które wprowadzamy w panelu logowania, np. jakiś aplikacji webowej. Jeżeli ta transmisja nie jest odpowiednio szyfrowana, to osoba postronna lub wyspecjalizowane narzędzie może uzyskać wgląd w te dane i wykorzystać je przeciwko nam. W momencie, kiedy my nie będziemy monitorować tej naszej sieci, to prędzej czy później zrobi to ta postać symbolizująca cyberprzestępcę, której celem może być m.in. eksfiltracja naszych danych. Mało tego, to w takich okolicznościach ta postać może mieć długotrwały dostęp do naszej sieci, a my nie będziemy mieli o tym wiedzy. Uwaga ta kierowana jest głównie do mniejszych podmiotów, które w swojej infrastrukturze posiadają kilka lub kilkanaście komputerów i nie sprawują kontroli nad przepływem danych tej sieci. Myślę, że duże podmioty, zwłaszcza te, które zostały objęte ustawą o Krajowym Systemie Cyberbezpieczeństwa, a w szczególności operatorzy usługi kluczowej, zmierzyły się już z tą problematyką i stosują pewne rozwiązania techniczne. Natomiast dla pozostałych chciałem tutaj wyszczególnić pewne rozwiązania, które służą m.in. do monitorowania zdarzeń i anomalii występujących w sieciach lokalnych i powiadomienia o tym fakcie. Jednym z takich rozwiązań jest IDS, czyli Intrusion Detection System. Systemy tego typu mają za zadanie wykryć podejrzanе działania i generować alerty po ich wykryciu. Kolejnym rozwiązaniem tego typu może być IPS, czyli Intrusion Prevention System, który od IDS-a różni się tym, że może zablokować niepożądane działania w sieci. Innym urządzeniem, które możemy tu wyszczególnić jest Next Generation Firewall, czyli zaporę sieciową nowej generacji, która jest uzbrojona w dodatkowe funkcje, takie jak kontrola aplikacji, zintegrowane zapobieganie włamaniom i często bardziej zaawansowane funkcje zapobiegania zagrożeniom, takie jak chociażby Sandbox, czyli piaskownica. Do tematu Sandbox jeszcze wrócimy w tej prezentacji. Kolejnym urządzeniem może być, do tej grupy można zaliczyć serwery pośredniczące, takie jak proxy lub Secure Gateway. Rozwiązania te mogą dostarczać informacji o ruchu aplikacyjnym, ale ich głównym zadaniem jest zapewnienie bezpieczeństwa użytkownikowi internetu.

Warto również wspomnieć, że bardzo istotnym elementem jest ruch DNS, dzięki któremu możemy wykryć nie tylko połączenia do potencjalnie złośliwych domen, ale też warto wiedzieć, że wiele technik używanych przez atakujących jest przeprowadzanych za pomocą tego protokołu. A mowa tutaj np. o tunelowaniu, eksfiltracji danych oraz komunikacji z

zewnętrznymi serwerami Command and Control. Kolejnym istotnym elementem są Logi systemowe oraz Logi aplikacyjne. Można w nich znaleźć ogrom różnych zdarzeń np. uruchomione procesy, zalogowanie się do systemu, wykonane połączenia i temu podobne zdarzenia. Systemem, który agreguje różnego rodzaju Logi i zdarzenia występujące w sieci lokalnej, jest system klasy SIEM, czyli Security Information, and Event Management. Jest technologia, która pozwala na zarządzanie informacją i zdarzeniami bezpieczeństwa w obrębie naszej infrastruktury sieciowej. Na podstawie zbieranych danych system ten umożliwia monitorowanie i wykrywanie zagrożeń, zarządzanie incydentami bezpieczeństwa, jak również wsparcie procesu zgodności, czyli compliance.

Kolejnym wyszczególnionym jest EDR, czyli Endpoint Detection and Response, czyli system chroniący i monitorujący stację roboczą. Systemy tego typu posiadają m.in. możliwość rozpoznawania i blokowania wskaźników ataków w czasie rzeczywistym.

Kolejny to jest DLP, czyli Data Loss Prevention. Systemy te służą do wykrywania naruszeń bezpieczeństwa związanych z wyciekami danych, mogą analizować przesłane pliki, oraz ich zawartość w poszukiwaniu wrażliwych informacji, takie jak chociażby: numer PESEL, a także inne dane osobowe, które mogą stać się celem atakującego. Rozwiązania te zapewniają też ochronę przed przypadkowymi lub celowymi wyciekami informacji. Ostatnim tu z wymienionych jest Net Generation Antywirus, z uwzględnieniem architektury centralnie zarządzanej.

Przejdźmy teraz do zarządzania podatnościami. Ten temat również pojawiał się w Państwa zapytaniach. Warto wiedzieć, że podatność może dotyczyć aplikacji serwerów, a także urządzeń sieciowych. Informacji o podatnościach możemy szukać m.in. na podanej tutaj stronie cvedetails.com. Common Vulnerabilities and Exposures jest to słownik identyfikatorów odpowiadających powszechnie znanych podatnościom oraz zagrożeniom, a także standard ich nazewnictwa. Możemy tu wyszukać zgłoszone podatności pod różnymi kryteriami takimi jak: identyfikator właśnie tego CVE, nazwa produktu, nazwa dostawcy oraz typ luki. Zachęcam Państwa do przeszukania tej bazy, wprowadzając nazwę sprzętu lub oprogramowania, które Państwo posiadają w swoich zasobach, w zasobach systemowych. Można się w ten sposób dowiedzieć, która wersja oprogramowania danego urządzenia posiada luki i zweryfikować to z oprogramowaniem zainstalowanym na swoim urządzeniu. Dodatkową funkcjonalnością tego portalu jest możliwość przeglądania wykrytych luk w zabezpieczeniach wg typu. Ja tu dokonałem takiego sprawdzenia, gdzie pokazuje nam trzy takie główne podatności, które zostały również sklasyfikowane w OWASP Top Ten, czyli Open Web Application Security Project. Na samej górze widzimy wykres podatności zwanej Execute Code, czyli wykonanie kodu. I widzimy, proszę Państwa jest tendencja. Praktycznie od 2013 roku mamy prawie nieprzerwany wzrost wykrywalności tych podatności. Także proszę zobaczyć, jak to wszystko wygląda pod tym kątem.

Kolejną podatnością jest Cross Site Scripting, który też ma bardzo podobną tendencję, również jak widać wzrostową. No i to, co jest najbardziej zastanawiające, to podatność typu SQL Injection. Mówiło się swojego czasu, że ta podatność jest już tak opanowana, że tu nie powinno, prawda, być nowych jakiś tam, nowych wykryć tego typu podatności. Jednak widzimy, że w

ostatnim czasie nastąpił wzrost tych właśnie zgłoszeń tego rodzaju podatności. Także myślę, że to daje domyslenia. Tu z kolei na tym wykresie chciałem przede wszystkim zasygnalizować ogólną tendencję wzrostu wykrywanych podatności. Także widzimy, że do 2020 mieliśmy tam około 20 tys. różnych wykrytych tych podatności. A już w tym roku mamy około, chyba tam, 17 tys., a że zostało nam jeszcze kilka miesięcy, no to teraz pytanie, czy przejdziemy, czy tych wykryć w tym roku będzie więcej. Ale myślę, że warto mieć świadomość tego typu, że jest taka tendencja wzrostowa.

Teraz proszę Państwa, przechodzimy sobie do zagadnienia oprogramowania. Też było wiele pytań temat, jakie oprogramowanie można w ogóle stosować? Czy wszystko co za darmo, możemy sobie zainstalować? Czy są jakieś wytyczne przede wszystkim do tego, jak to oprogramowanie może funkcjonować. I tutaj chciałbym, szczególnie polecić Państwu właśnie ten link, pod którym znajdują się wytyczne takie jak Narodowe Standardy Cyberbezpieczeństwa, gdzie zostały właśnie opracowane różne wytyczne. Ja tutaj wskazałem dwa przykładowe. Minimalne wymagania bezpieczeństwa informacji, jak również zabezpieczenie ochrony prywatności systemów informatycznych oraz organizacji. Polecam właśnie zweryfikować te wszystkie zagadnienia, które stanowią zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych, wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. Musimy mieć świadomość, że Narodowe Standardy Cyberbezpieczeństwa zostały opracowane na podstawie standardów amerykańskiego National Institute of Standards and Technology, czyli NIST. I co ciekawe zostały przyporządkowane obowiązującym w Polskim Systemie Prawnym normom stosowanym w Zarządzaniu Bezpieczeństwem Informacji przez podmioty Krajowego Systemu Cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne operatorów usług kluczowych i dostawców usług cyfrowych. Na standardy te składa się tutaj proszę Państwa kilkanaście, dosłownie dokumentów. Zachęcam Państwa do zapoznania się właśnie z tą całą listą. Wspomnę tylko, że standardy te obejmują m.in. cyberbezpieczeństwo chmur obliczeniowych. Także myślę, że to jest ciekawe zagadnienie. Dobrze, jeżeli chodzi o oprogramowanie, proszę Państwa, to czy możemy sobie instalować, czy nie, to zależy głównie tak naprawdę od licencji. To w licencji musimy zweryfikować, czy producent zezwala na instalację oprogramowania w celach, czy to domowych, czy może być wykorzystywany również w celach komercyjnych. Jeżeli już ustalimy, że licencja zezwala na korzystanie z tego oprogramowania, to pamiętajmy, że przy pobieraniu tego oprogramowania, jeżeli taka możliwość - często jest, bo producenci zamieszczają tzw. sumy kontrolne, które służą do weryfikacji, czy to oprogramowanie nie zostało zmienione przez, może jakąś osobę, która się podszyła, która generalnie zmieniła to oprogramowanie. Także zalecam weryfikację tych sum kontrolnych.

Kolejnym punktem, na które należy zwrócić uwagę, jest reputacja źródła. Otóż, jeżeli sobie wpisujemy nazwę pożądanego przez nas oprogramowania, w wyszukiwarce i korzystamy z pierwszego lepszego tzw. linku, no to może się okazać, że to nie jest tak naprawdę strona producenta i pobieramy oprogramowanie, które może zostało w pewien sposób zmodyfikowane. Także zalecam dużą ostrożność przy pobieraniu tych programów. Teraz tak, co możemy zrobić z tak pobranym oprogramowaniem, w jaki sposób możemy sprawdzić.

Pamiętajmy, że przede wszystkim, pamiętajmy, że każde programowanie i aplikacje na dzień dzisiejszy można spreparować, podszyć się właśnie z wykorzystaniem spoofingu. Dotyczy to głównie aplikacji, web aplikacji w szczególności, gdzie cyberprzestępca może podmienić panel logowania, w taki sposób, że Państwo wprowadzają swoje dane uwierzytelniające i te dane trafiają do cyberprzestępcy, ale też przesyłane właśnie na ten rzeczywisty portal, czyli następuje to logowanie. I tu jest to niebezpieczeństwo, że nawet Państwo mogą nie zauważyć, że te dane zostały przekazane gdzieś poza tym oficjalnym kanałem. Najczęściej podatność tego typu będzie występowała w przypadku, kiedy logujemy się na stronach innych niż strony rzeczywiste. Ktoś zapyta, czy może występować taki problem przy logowaniu na stronę rzeczywistą, czy można gdzieś nas w jakiś sposób przekierować. Odpowiadam, że tak niestety można. Występuje to przy ataku typu Arp Spoofing, gdzie zostaje podmieniony ten adres, prawdziwy adres zostaje podmieniony adres atakującego. Kiedy się taka sytuacja może wydarzyć, chociażby wtedy, kiedy nie monitorujemy działań w naszej sieci i dopuścimy po prostu do powstania takiego ataku. Także jeszcze raz tutaj zwracam uwagę na monitorowanie sieci, to jest bardzo istotny temat.

Teraz proszę Państwa, przejdziemy sobie takiego zagadnienia. Jeżeli sobie pobierzemy już ten plik, czy możemy właśnie zweryfikować ten plik instalacyjny, który, czy został w jakiś sposób doposażony, tak to nazwijmy, w złośliwy kod. Możemy to zweryfikować z wykorzystaniem właśnie takiego systemu Virustotal.com. I na tej stronie istnieje możliwość właśnie przesłania takiego pliku. Ja tutaj dokonałem takiego próbnego właśnie testu, gdzie przesłałem plik test.txt. Został on określony jako pliki JavaScript, ale tak jak widzimy 58 silników antywirusowych, które zweryfikowało ten plik, stwierdziło że rzeczywiście nie ma tutaj zagrożeń. Także jest jakieś rozwiązanie, które możemy właśnie zastosować, jeżeli nie jesteśmy pewni pliku, który pobierzemy. Możemy w ten sposób weryfikować oczywiście wszystkie pliki, z tym, że jest bardzo ważna uwaga. W momencie, kiedy weryfikujemy taki plik musimy mieć świadomość tego, że ten plik jest przesyłany na ten serwer. I on już tam po prostu zostaje. Także, jeżeli przesyłamy pliki, które zawierają jakieś dane poufne, no to niestety, ale to tak jak byśmy doprowadzili do wycieku danych. Także naprawdę musimy tutaj bardzo uważać, a musimy też wiedzieć, że serwis ten umożliwia komercyjny dostęp, gdzie osoby, które się zalogują do tego serwisu, mogą sobie te wszystkie pliki pobrać. Także zwracałbym szczególną uwagę na to, żeby nie przekazywać danych poufnych w ten sposób. Teraz ktoś zapyta, czy jest konieczność przesyłania takiego pliku. Odpowiadam, że niekoniecznie, bo można również zweryfikować plik, zwłaszcza jakiegoś oprogramowania, które jest takie powszechnie dostępne, przez wygenerowanie hasza tego pliku i przesłania tylko samego hasza. Także, jeżeli już był przesłany wcześniej taki plik no to będziemy mogli w ten sposób zweryfikować to oprogramowanie.

Kolejną metodą na weryfikację plików pod kątem bezpieczeństwa jest chociażby takie środowisko, właśnie tego Sandboxa, dostępnego chociażby z poziomu tutaj serwisu Any Run, gdzie możemy właśnie przesłać ten plik, i po założeniu konta i zalogowaniu się zobaczyć, jak w ogóle zachowuje się ta aplikacja w środowisku testowym. Jeżeli będą, jeżeli okazałoby się, że plik będzie zainfekowany, oczywiście Państwo zostaną o tym fakcie poinformowani przez ten portal. Zwracam tutaj jedynie uwagę, że tego typu środowisko powinno być uruchamiane

przede wszystkim w odizolowanym środowisku, najlepiej wirtualnym. Żebyśmy po prostu nie zainfekowali sobie pozostałej części sieci w ten sposób, jeżeli będziemy coś takiego weryfikować. Także zalecam dużą ostrożność, jednocześnie korzystanie właśnie z tego typu środowisk odizolowanych.

Teraz przechodzimy do zagadnień zabezpieczenia poczty elektronicznej. Ten temat również przewijał się w zapytaniach. Myślę, że już wszyscy mamy świadomość, jak bardzo poczta elektroniczna jest ważnym elementem w funkcjonowaniu naszych działalności. Jak łatwo tak naprawdę, dostać się do nas, do naszych zasobów, do organizacji właśnie w ten sposób. Pamiętajmy, że wysyłanie poczty przede wszystkim funkcjonuje na podstawie protokołu SMTP, czyli Simple Mail Transfer Protocol. I tutaj słowo klucz - Simple -, tak to ten protokół został opracowany bodajże w latach osiemdziesiątych i miało być prosto. No i okazuje się, że ta właśnie funkcjonalność jest w tym momencie wykorzystywana chociażby do eMail spoofingu, czyli cyberprzestępca może się podszyć, bardzo łatwo może się podszyć generalnie, w momencie, kiedy serwer pocztowy jest niezabezpieczony, bardzo łatwo może się podszyć właśnie pod nadawcę tej poczty. No i tutaj rekomendowanymi rozwiązaniami technicznymi są właśnie, tak jak tutaj wyszczególniłem te trzy elementy, czyli SPF, DKIM, DMARC. Nie będziemy się tutaj zagłębiać w te szczegóły techniczne, natomiast warto wiedzieć, że te elementy mają zapobiegać przede wszystkim właśnie temu zjawisku eMail spoofingu. Ze swojej strony jeszcze dodam, że dobrze jest, kiedy nie polegamy tylko na danych uwierzytelniających, typu login, hasło. Dobrze jest jeszcze doposażyć właśnie funkcjonowanie takiej poczty, chociażby przez Two Factor Authentication, czyli dwuskładnikowe uwierzytelnianie. I teraz jeszcze ważna uwaga, proszę Państwa. Czasami dojdzie już do przełamania tych zabezpieczeń naszej poczty. Dlatego warto jest weryfikować, co my na tej poczcie elektronicznej tam przechowujemy, jakie dokumenty. Musimy mieć świadomość, że jeżeli osoba atakująca dostanie się do tej poczty i będzie mogła sobie wyczytać tam różne informacje, czy o nas, czy o naszych kontrahentach, z którymi współpracujemy, to bardzo łatwo będzie mogła spreparować takiego maila. Także zwracajmy uwagę na zawartość naszych skrzynek pocztowych.

Kolejny temat, który się pojawiał w zapytaniach od Państwa były warunki, w jakich należy skonfigurować środowisko domowe do pracy zdalnej. Myślę, że najlepszym wskazaniem jest tutaj właśnie ten przewodnik, "Po telepracy w podmiocie publicznym", który został właśnie również wyszczególniony w Narodowych Standardach Cyberbezpieczeństwa i jest dostępny właśnie tam na tej stronie internetowej, którą Państwu prezentowałem. Ze swojej strony dodam tylko, tyle, że warto zadbać o to, żeby te transmisje, jeżeli łączymy się z domu, żeby ta transmisja odbywała się przez tunelowanie z wykorzystaniem kryptografii. Czyli tak naprawdę mowa tu o VPN, który powinien być odpowiednio dobrany przez organizację. Warto też zwracać uwagę na segmentację sieci. Czyli, jeżeli w sieci domowej mamy inne komputery i one mogłyby w jakiś sposób wpłynąć na nasz kanał, na nasze środowisko, dobrze jest po prostu się odizolować właśnie w ten sposób przez stosowanie właśnie tej segmentacji sieci. No oczywiście element niezbędny, aktualizacja oprogramowania urządzeń, które posiadamy w domu i łączymy się przez nie. Myślę tutaj o routerze. Zweryfikujmy czy rzeczywiście ten software, czyli oprogramowanie tego routera jest aktualizowane. No i tutaj teraz taka mała

podpowieć, bo jeżeli się okaże, że na tym routerze to oprogramowanie już dawno jest nieaktualizowane, zweryfikujemy, czy przypadkiem nie ma możliwości zmiany tego oprogramowania, chociażby Open WRT, to takie alternatywne oprogramowanie, które często pozwala na wykorzystanie dodatkowych funkcjonalności nawet naszych routerów domowych. Z tym, że tu też bardzo ważna uwaga. Jeżeli chcemy zainstalować tego typu firmware, zweryfikujemy wcześniej licencję urządzenia, czy w ogóle producent pozwala nam na takie działania. Także polecam, tego typu rozwiązania.

Kolejnym tematem, który pojawił się w zapytaniach, był temat dotyczący szkoleń. W jaki sposób, czy sprawdzać, czy weryfikować pracowników, czy można takie rzeczy robić. Proszę Państwa ja ze swojej strony mógłbym tutaj podać taki przykład, gdzie na kanale Warszawskiego Instytutu Bankowości są nagrane, takie właśnie krótkie filmiki, przez znanych polskich aktorów Panią Ewę Kasprzyk, Pana Cezarego Pazury. Publikują po prostu, w jaki sposób trzeba w tej cyberprzestrzeni się poruszać. Także polecam, jeżeli ktoś szuka inspiracji do tworzenia właśnie szkoleń tego typu polecam właśnie ten kanał.

I teraz druga część się zapytania, czyli właśnie, czy można w ogóle weryfikować pracowników pod kątem, czy właściwie zrozumieli przede wszystkim ten przekaz szkoleń. No i chciałbym tutaj właśnie wskazać taki serwis canarytokens.org, gdzie Państwo mogą sprawdzić, którzy pracownicy nie przestrzegają zasad bezpieczeństwa, a wystarczy wygenerować spreparowany plik np. Worda, Excela, czy też jakąś stronę www i wysłać taki plik z nieznanego adresu e-mail i za każdym razem, gdy pracownik otworzy taki załącznik, otrzymają Państwo powiadomienie o tym fakcie. Także można to w taki dosyć łagodny sposób zweryfikować, którzy z naszych pracowników jeszcze otwierają jakieś nieznane linki. Dobrze, proszę Państwa, przechodzimy do ostatniego zagadnienia, jakim są informacje w sieci. Musimy mieć świadomość, że dzisiaj wszystkie informacje, które są zamieszczane na stronach internetowych, czy to jest treść pisana, czy to są nawet jakieś formy audiowizualne, mogą zostać w bardzo łatwy sposób zmienione i zmodyfikowane. I myślę, że najlepiej ten element został przedstawiony właśnie w filmie dokumentalnym "The Great Hack", czyli hakowanie świata. Jest to film dokumentalny 2019 roku, który ujawnił kulisy afery z Cambridge Analytica, gdzie właśnie została wykorzystana duża ilość danych osobowych pozyskanych w sposób nielegalny. Nie będę tutaj spojlerował. Zachęcam Państwa do obejrzenia tego filmu. Natomiast, tak na zakończenie, chciałbym przekazać tylko jedno zdanie z tego filmu "nie sposób rozróżnić, co jest czym, bo nic nie jest tym, czym się wydaje".

Dziękuję Państwu za uwagę.