Transkrypcja webinaru „**Jak zapobiegać i radzić sobie z cyberzagrożeniami, czyli firma bezpieczna cyfrowo**”, zorganizowanego 3 grudnia 2024 w ramach projektu Digital Biznes.

red. Natalia Kieszek:

Dzień dobry, witam Państwa bardzo serdecznie. Nazywam się Natalia Kieszek i mam przyjemność poprowadzić dzisiaj drugi webinar Ministerstwa Rozwoju i Technologii, tym razem poświęcony cyberbezpieczeństwu i cyber zagrożeniom, bo już co piąty polski pracownik w miejscu pracy padł ofiarą cyberataku, a niewiele ponad połowa firm używa oprogramowania antywirusowego. Cyberzagrożenia dotyczą każdego, nie tylko przedsiębiorcy, ale również każdego pracownika, niezależnie od wielkości firmy czy też branży, w której działa. Dlatego tak ważny jest świadomy i przeszkolony pracownik, a nie tylko narzędzia, z których korzysta dzisiaj. Ministerstwo Rozwoju i Technologii połączyło siły z NASK, aby przedstawić małym i średnim firmom narzędzia, których można używać i zachować cyberbezpieczeństwo w firmie. Dzisiaj ze mną w studiu są eksperci do spraw Cyberbezpieczeństwa w NASK Pani Anna Kwaśnik i pan Piotr Ławniczak. Zanim oddam głos tutaj naszym gościom w studiu chciałabym tylko przypomnieć, że podczas dzisiejszego wydarzenia. Można oczywiście zadawać pytania na czacie. Później zadamy je oczywiście naszym ekspertom. A na koniec zachęcamy do wypełnienia ankiety jak dzisiejszy webinar Wam się podobał. Przypominam jeszcze, że zapraszamy na spotkania stacjonarne, które odbędą się 4 grudnia i 12 grudnia w Centrum Przedsiębiorczości Smolna. A tymczasem oddaję już głos naszym prelegentom. Zaczynamy dzisiaj od prezentacji pani Anny.

Anna Kwaśnik:

Dzień dobry, witam Państwa bardzo serdecznie. Podczas dzisiejszego spotkania chciałabym zwrócić uwagę. Czym jest cyberbezpieczeństwo i dlaczego my jako pracownicy, pracodawcy i przedsiębiorcy powinniśmy zadbać o cyberbezpieczeństwo i dlaczego tak ważne jest szkolenie naszych pracowników, ale także podnoszenie swoich własnych kompetencji. Podczas dzisiejszego spotkania pokrótce przypomnę Państwu, czym jest cyberbezpieczeństwo, a także takie pojęcia jak cyberodporność i odporność systemów teleinformatycznych. Pokrótce przedstawię liczby, które pokazują, z czym pracownicy i przedsiębiorcy borykają się na co dzień. Opowiem też o cyber pułapkach, na które narażeni jesteśmy my jako pracownicy. A

także dam wskazówki o tym, jak dbać o naszą cyber świadomość oraz podstawowe zasady cyber higieny. Przede wszystkim zacznijmy od tego, czym jest cyberbezpieczeństwo. Myślę, że tutaj większość z Państwa doskonale wie, że zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, cyberbezpieczeństwo definiujemy jako wszystko to, co wpływa na odporność systemów teleinformatycznych, które może naruszać autentyczność, poufność, integralność i dostępność danych, które przetwarzane są przez systemy teleinformatyczne.

Niezwykle ważne jest to, abyśmy my jako pracodawcy, pracownicy i osoby związane z Krajowym Systemem Cyberbezpieczeństwa dbali o odporność naszych systemów teleinformatycznych, a także dbali o cyberodporność. Zanim opowiem, jak budować cyberodporność naszej organizacji, przede wszystkim pamiętajmy to. Czym jest cyberodporność? Gdybyśmy się pogłębili nad tym, nad tą definicją to nic innego jak przygotowanie danej organizacji na to, jak sobie radzić z atakiem cybernetycznym, na który tak naprawdę narażony jest każdy z nas. Niezwykle ważne jest to, aby nasza organizacja, firma czy też nasze przedsiębiorstwo potrafiło zapewnić ciągłość działania. Jeżeli będziemy mieli styczność z atakiem cybernetycznym. To w jaki sposób budować tą cyberodporność naszej organizacji. To przede wszystkim właściwe przygotowanie się na to. Niezwykle ważne jest, aby w naszej organizacji stworzyć takie procedury i ułożyć tak procesy związane z ciągłością działania, aby rzeczywiście po wystąpieniu ataku nasza firma mogła funkcjonować dalej. Ważne jest aby stosować takie narzędzia, które zapewnią nam ciągłość procesów i ciągłość działania, bo jak się później okaże, na ataki cybernetyczne narażony jest każdy z nas.

Gdy mówimy o cyberodporności, musimy także pamiętać o budowaniu kompetencji wśród naszych pracowników, a także o nas samych w taki sposób, abyśmy wiedzieli, jak się zachować w danej sytuacji, co zrobić oraz jak reagować na różnego rodzaju cyberataki. Teraz wróćmy do odporności systemów teleinformatycznych. Dbałość o to jest niezwykle istotna, zwłaszcza gdy mówimy o cyberbezpieczeństwie w kontekście ustawy o KSC. Każda organizacja, każda firma, każda jednostka powinna zadbać o bezpieczeństwo sieci teleinformatycznych, które używane są w naszej organizacji, aby budować cyberodporność systemów teleinformatycznych. Musimy także pamiętać, że musimy to robić wielopoziomowo. Nie tylko bezpieczeństwo sieci teleinformatycznych, ale także bezpieczeństwo urządzeń i narzędzi, z których korzystamy, gdy mówimy o narzędziach w naszej instytucji, w naszej placówce, w naszej firmie. Mówimy także o oprogramowaniu i aplikacjach, z których korzystamy. Dbałość o nie jest niezwykle istotna i niezwykle potrzebna, aby odporność naszych systemów rzeczywiście była na wysokim poziomie. I pamiętajmy, że żadne procedury, żadne narzędzia i żadne rozwiązania nie będą

skuteczne, jeśli nie będziemy dbali o właściwe kompetencje naszych pracowników, jeśli nie wprowadzimy odpowiednich procedur i praktyk obowiązujących w naszej organizacji.

Gdy mówię tutaj o praktykach obowiązujących w organizacji, pamiętajmy, jak niezwykle ważne jest to, aby stale podnosić świadomość naszych pracowników i nas samych na temat różnych zagrożeń. Jak się okazuje, każdy z nas jest na nie narażony, a cyberprzestępcy stale doskonalą swoje metody i praktyki. Tak naprawdę każdy z nas może doświadczyć cyberataku. Gdybyśmy teraz pochylili się nad obrazem cyberbezpieczeństwa wśród pracowników w naszym kraju, warto zwrócić uwagę na badania przeprowadzone przez firmę Dogma Bezpieczeństwo IT i ESET. Przeprowadzone przez nich badania pokazują, jak pracownicy radzą sobie z różnymi cyberzagrożeniami w Polsce. Więcej o krajobrazie cyberbezpieczeństwa opowie później kolega. Natomiast teraz chciałabym przedstawić, co dzieje się wśród pracowników. Zgodnie z przedstawionym raportem, aż jeden na pięciu pracowników padł ofiarą cyberataku w organizacji. Co ciekawe, aż jeden na trzech pracowników zna kogoś, kto doświadczył tego typu działań cyberprzestępczych. Warto zwrócić też uwagę na to, co się dzieje i jakie są typy incydentów wśród pracowników różnych firm i organizacji.

Przede wszystkim aż 32% pracowników otrzymało alert z programu antywirusowego informujący o potencjalnym zagrożeniu. Co ciekawe, 34% respondentów przyznało, że zna osobę, która doświadczyła cyberataku podczas wykonywania obowiązków służbowych. Ponadto aż 47% pracowników różnych firm i organizacji otrzymało nietypową wiadomość, której nie wykryły rozwiązania technologiczne ani filtry antyspamowe, i która potencjalnie mogła być wiadomością phishingową. Gdybyśmy chcieli bliżej przyjrzeć się, na jakie typy incydentów napotykają pracownicy, są to przede wszystkim wiadomości z niebezpiecznego źródła, telefony z nieznanych numerów – zarówno krajowych, jak i zagranicznych – oraz różnego rodzaju alerty z programów antywirusowych. Często są to również informacje o zainfekowaniu służbowego sprzętu szkodliwym oprogramowaniem. Wśród incydentów wymienia się także włamania do firmowych systemów, kradzież tożsamości czy też haseł. Przedstawione badania pokazują, że niestety każdy pracownik – każdy z nas, kto korzysta z Internetu i ma styczność z nowymi technologiami – musi liczyć się z ryzykiem potencjalnego cyberataku. Tego rodzaju zagrożenia mogą być bardzo niebezpieczne i przynieść poważne skutki zarówno dla nas samych, jak i dla naszych organizacji.

Gdy mówimy o cyberzagrożeniach i cyberatakach, na które narażeni jesteśmy zarówno jako codzienni użytkownicy internetu, jak i pracownicy, często mamy na myśli ataki związane z

socjotechniką. Socjotechnika, w kontekście różnego rodzaju oszustw i przestępstw komputerowych, nazywana jest również inżynierią społeczną. Jest to zbiór działań mających na celu nakłonienie nas do podjęcia określonych działań, które najczęściej prowadzą do wykradzenia danych osobowych lub finansowych. Przestępcy stosują różnorodne metody, kontaktując się z nami na wiele sposobów – poprzez podejrzane wiadomości e-mail, SMS-y, połączenia telefoniczne czy inne formy komunikacji. Codziennie jesteśmy narażeni na takie działania. W metodach socjotechnicznych cyberprzestępcy najczęściej wykorzystują nasze emocje, takie jak lęk, stres czy strach. Przykładem są wiadomości lub informacje sugerujące, że coś niepokojącego dzieje się na naszym koncie, albo że musimy natychmiast podjąć działania, często w kontekście biznesowym.

Cyberprzestępcy bardzo często wykorzystują wpływ autorytetu, podszywając się pod naszego pracodawcę, szefa lub inną osobę na wyższym stanowisku, która zleca wykonanie konkretnego zadania. Zazwyczaj działają tak, aby wymusić na nas natychmiastową reakcję. Działania te są przedstawiane jako pilne i wymagające niezwłocznego wykonania – sugeruje się, że jeśli nie podejmiemy działania od razu, możemy na przykład utracić pracę lub nasza organizacja może ponieść poważne konsekwencje. Metody stosowane przez cyberprzestępców często wydają się nam znajome, a wielu z nas mogłoby stwierdzić, że nigdy nie dałoby się oszukać. Jednak łatwo jest tak mówić w bezpiecznych warunkach. Gdy w grę wchodzą silne emocje, obawy lub polecenia od przełożonych, nie zawsze potrafimy zachować zdrowy rozsądek, a nasza czujność może zostać uśpiona. Szczególnie niebezpieczne są ataki socjotechniczne, które opierają się na personalizacji. W takich przypadkach cyberprzestępcy dokładnie wiedzą, do kogo kierują swoje wiadomości, co znacznie zwiększa skuteczność ich działań.

O ile większość z nas traktuje wiadomości o opłaconej fakturze czy dopłacie do paczki z przymrużeniem oka i niewielu z nas daje się na nie nabrać, sytuacja wygląda inaczej, gdy otrzymujemy wiadomość imienną. Gdy wiadomość zawiera dokładne informacje o stanowiskach w naszej firmie lub odnosi się do wydarzeń mających miejsce w naszej organizacji, nie zawsze potrafimy podejść do niej racjonalnie. Niestety, zdarza się, że w takich sytuacjach ulegamy oczekiwaniom cyberprzestępców. Tematy związane z phishingiem i zagrożeniami wynikającymi z socjotechniki są tak obszerne, że można by o nich przeprowadzić wiele webinarów, a temat wciąż by się nie wyczerpał. Jednak podczas dzisiejszego spotkania chciałabym zwrócić uwagę na szczególne rodzaje zagrożeń, na które Wy – jako pracownicy i przedsiębiorcy – jesteście szczególnie narażeni. Chciałabym przybliżyć zagrożenie związane z tak zwanym spersonalizowanym atakiem phishingowym, znanym również jako atak typu BEC (Business

Email Compromise) lub oszustwo na dyrektora. Jak przebiega taki atak i dlaczego jest szczególnie niebezpieczny? Atak rozpoczyna się od tego, że cyberprzestępca zbiera szczegółowe informacje o nas, naszej firmie, naszych pracownikach oraz zależnościach służbowych. Dzięki temu jest w stanie przygotować wiarygodną i przekonującą wiadomość, która znacznie zwiększa szansę na sukces jego działań.

Dzięki temu cyberprzestępcy są w stanie przygotować wiadomości e-mail, które wyglądają na autentyczne i wskazują osoby zajmujące kluczowe stanowiska w organizacji. Zdarza się, że przestępcy zdobywają dostęp do naszej poczty lub poczty naszych współpracowników, co pozwala im przeprowadzić wiarygodne rozmowy, mające na celu skłonienie nas do podjęcia określonych działań. Kiedy zdobędą już potrzebne informacje, a być może nawet dostęp do naszych wiadomości e-mail, dokładnie analizują sposób, w jaki się komunikujemy. Na tej podstawie przygotowują fałszywe wiadomości, które mogą być wysyłane zarówno za pośrednictwem e-maila, jak i komunikatorów. Bardzo często w takich wiadomościach wykorzystują wizerunek naszego przełożonego lub kontrahentów, wywierając presję czasu i nakłaniając nas do natychmiastowego działania. Najczęściej tego typu wiadomości zmuszają nas do szybkiego podjęcia decyzji, takich jak natychmiastowe dokonanie płatności, pobranie załącznika lub zmiana numeru konta bankowego na fakturze, na którą mamy przelać pieniądze. Dodatkowo cyberprzestępcy, powołując się na stanowisko dyrektora lub prezesa organizacji, często proszą o zachowanie poufności. Dla wielu z nas, jako pracowników, taki element może sprawiać, że wiadomość wydaje się jeszcze bardziej wiarygodna, co z kolei wpływa na sposób, w jaki ją traktujemy.

Co możemy zrobić jako pracownicy i jak często reagujemy na tego typu sytuacje? Przede wszystkim fakt, że wiadomość wygląda autentycznie, pochodzi rzekomo od naszego prezesa lub nadawca wydaje się być osobą, za którą się podaje, sprawia, że często podejmujemy działania, o które proszą nas cyberprzestępcy. W kontekście ataków typu BEC warto przytoczyć przykład, który miał miejsce kilka miesięcy temu. Policja z Hongkongu opisywała przypadek oszustwa, w którym cyberprzestępcy wykorzystali nowe technologie, w tym deepfake, i w podstępny sposób wyłudzili od jednego z pracowników ponad 25 milionów dolarów. Choć brzmi to jak scenariusz z filmu, sytuacja miała miejsce naprawdę. Jak wspomniałam wcześniej, cyberprzestępcy stale udoskonalają swoje metody. W tym przypadku zastosowali technologię deepfake, aby uwiarygodnić oszustwo. Pracownik, który otrzymał informację o konieczności dokonania kilku przelewów, początkowo zachował się prawidłowo – podszedł do sprawy z dystansem i próbował zweryfikować, czy wiadomość jest prawdziwa.

Gdy pracownik połączył się z zarządem podczas wideokonferencji, zarówno obrazy, jak i głosy osób uczestniczących w rozmowie wydawały się całkowicie autentyczne. Niestety, pracownik dał się nabrać i dokonał przelewów zgodnie z instrukcjami. Być może wielu z Was zastanawia się, dlaczego nie rozpoznał, że obraz był deepfake. Czy nie zauważył zakłóceń w głosie? Pamiętajmy, że podczas wideokonferencji jakość obrazu i dźwięku nie zawsze jest idealna. Zakłócenia w transmisji są czymś normalnym, zwłaszcza gdy rozmowy odbywają się z osobami znajdującymi się w innym kraju czy mieście. W tym przypadku nic nie wzbudziło podejrzeń pracownika. Choć ta historia może wydawać się nieprawdopodobna, być może część z Was myśli, że coś takiego nie zdarzy się w Waszej organizacji. Jednak warto pamiętać, że na tego typu oszustwa narażony jest każdy pracodawca i każdy pracownik. Dlatego tak istotne jest wprowadzenie w organizacji odpowiednich procedur i rozwiązań, które pozwolą zatrzymać proces zmiany numeru konta bankowego lub transferu pieniędzy, zanim dojdzie do nieodwracalnych konsekwencji.

Pamiętajmy, że konsekwencje ataku typu BEC (Business Email Compromise) mogą być bardzo różnorodne i dotyczyć wielu aspektów. Przede wszystkim może dojść do utraty środków finansowych – czasem są to ogromne kwoty. Dodatkowo cyberprzestępcy mogą wykradać nasze dane, udostępniać poufne informacje o firmie, zainfekować urządzenia lub całą sieć, z której korzystamy, a następnie żądać okupu w zamian za ich odblokowanie. W takich przypadkach może również dojść do kradzieży danych, co wiąże się z poważnymi konsekwencjami dla organizacji. Mówiąc o żądaniu okupu czy zaszyfrowaniu plików, chciałabym pokrótce opowiedzieć o atakach typu ransomware. Wiele osób zapewne słyszało o tego rodzaju oszustwach i przestępstwach. Mam nadzieję, że nikt z Państwa nie doświadczył tego na własnej skórze, jednak jest to realne zagrożenie, które może dotknąć zarówno pracowników, jak i codziennych użytkowników internetu. Jak dochodzi do ataków typu ransomware? Przede wszystkim przez pobranie zainfekowanych plików. Mogą one pochodzić z wiadomości e-mail lub wiadomości przesyłanych za pośrednictwem komunikatorów. Innym sposobem jest wejście na zainfekowane strony internetowe, które mogą wprowadzić złośliwe oprogramowanie na nasze urządzenia.

To też słabe hasła i słabe zabezpieczenia, jakie stosujemy w naszej firmie, które umożliwiają cyberprzestępcom dotarcie do naszej firmy, które umożliwiają im wtargnięcie do naszej sieci, ale także różnego rodzaju zaniedbania z naszej strony. Zaniedbania takie jak. Nieaktualizowanie systemów i urządzeń i aplikacji, z których korzystamy. Pamiętajmy, że

ransomware to złośliwe oprogramowanie, które powoduje blokadę i blokadę dostępu do danych, które przetwarzamy w naszej organizacji. W zamian za odblokowanie tego musimy zapłacić okup. Musimy spełnić żądania cyberprzestępców. Żądania te bardzo często są na bardzo wysokich, są w bardzo wysokich kwotach i niestety wielu pracowników, wielu pracodawców, wielu przedsiębiorców się na to zgadza. Jednym z takich najpopularniejszych przykładów ataku typu ransomware, który myślę, że być może dotknął i państwa, jest atak z 2023 roku, który dotknął firmę AlaP, wskutek której miliony czy setki tysięcy danych pacjentów i osób, które korzystały z usług labu, wyciekły do internetu. Gdybyśmy się zastanowili, co zrobić, gdy padniemy ofiarą tego typu ataku? Przede wszystkim pamiętajmy, żeby nigdy nie płacić okupu. Jeśli zapłacimy okup, tak naprawdę nie mamy pewności, czy dane, które zostały nam wykradzione, przede wszystkim zostaną odblokowane, ale również to, czy nasze dane nie zostaną udostępnione.

Gdy mówimy o zagrożeniach i cyberprzestępstwach, niezwykle istotne jest, jak my – pracownicy, przedsiębiorcy, a także właściciele mniejszych i większych firm – podchodzimy do budowania cyberświadomości w naszych organizacjach. Przykłady, o których wspomniałam, opierają się głównie na błędach ludzkich, które pracownicy popełnili w wyniku braku odpowiednich procedur czy wsparcia. Pamiętajmy, że każdy z nas może paść ofiarą tego typu ataku. Fakt, że pracownik lub my sami daliśmy się nabrać i kliknęliśmy w niewłaściwy link, nie świadczy o winie tego pracownika, lecz o niedostatkach w organizacji – brakujących procedurach, szkoleniach lub narzędziach wspierających bezpieczeństwo. Jednym z kluczowych elementów ochrony firmy przed zagrożeniami jest budowanie cyberświadomości wśród pracowników oraz w samej organizacji. Ważne jest, aby już od początku istnienia firmy wdrażać rozwiązania podnoszące świadomość zagrożeń oraz promujące najlepsze praktyki w zakresie cyberbezpieczeństwa. Kluczowe znaczenie ma wprowadzenie jasno określonych polityk bezpieczeństwa, które pozwolą na podniesienie poziomu cyberświadomości wśród pracowników. Dzięki temu wzmocnimy odporność organizacji na ataki, zwiększymy bezpieczeństwo danych i zminimalizujemy ryzyko popełniania błędów w przyszłości.

Pamiętajmy, aby od samego początku w naszej organizacji czy firmie dbać o kulturę bezpieczeństwa. Ważne jest, aby regularnie rozmawiać o cyberbezpieczeństwie, organizować spotkania, szkolenia oraz akcje uświadamiające, a także celebrować kulturę bezpieczeństwa jako integralny element naszej działalności. Nie należy bać się inwestycji w bezpieczeństwo. Choć dla wielu może to wydawać się wyzwaniem, często myślimy: „Mnie to nie dotyczy.” Jednak warto pamiętać, że koszty związane z inwestycją w cyberbezpieczeństwo są zawsze

mniejsze niż te, które poniesiemy w wyniku skutecznego cyberataku. Budowanie cyberświadomości powinno być procesem długofalowym i wielopoziomowym. Jeśli organizujemy szkolenia czy akcje uświadamiające, zadbajmy o to, aby odbywały się one regularnie i cyklicznie. Jednym z kluczowych momentów, w których szczególnie warto wdrażać działania edukacyjne, jest rozpoczęcie pracy przez nowych pracowników. To idealny czas, aby zadbać o ich cyberświadomość i podstawową wiedzę z zakresu cyberhigieny. Podobnie, jeśli sami rozpoczynamy działalność, powinniśmy od razu wprowadzić rozwiązania wspierające bezpieczeństwo i świadomość zagrożeń w naszej organizacji.

Pamiętajmy, że szkolenie pracowników nie powinno być jednorazowym wydarzeniem, o którym później zapominamy. Takie szkolenia powinny odbywać się cyklicznie – raz, dwa, a nawet trzy razy w roku. Ważne jest, aby stale przypominać o zagrożeniach i zasadach bezpieczeństwa.
Istnieje wiele narzędzi i rozwiązań, z których możemy korzystać, aby zwiększać świadomość pracowników. Często są to darmowe opcje, takie jak dzisiejsze spotkanie, podczas którego możecie dowiedzieć się o różnego rodzaju zagrożeniach oraz narzędziach ochrony dla swojej organizacji. Cyberświadomość i bezpieczeństwo organizacji nie mogą funkcjonować bez przestrzegania podstawowych zasad cyberhigieny. Tak jak w codziennym życiu dbamy o higienę osobistą, tak samo, korzystając z nowych technologii i narzędzi, powinniśmy dbać o higienę w cyberprzestrzeni. Cyberhigiena obejmuje wszystkie działania, które podejmujemy w celu zwiększenia bezpieczeństwa organizacji. To także świadomość tego, w jaki sposób działamy, jakie są obecne zagrożenia w cyberprzestrzeni i co możemy zrobić, aby ich uniknąć. Właściwa cyberhigiena pozwala nam chronić zarówno dane organizacji, jak i nasze własne.

Jednym z podstawowych elementów cyberhigieny są rozwiązania związane z hasłami dostępowymi do różnych usług. Tak jak w codziennym życiu, wychodząc z domu, zamykamy drzwi, aby chronić swoje mieszkanie, tak samo powinniśmy dbać o bezpieczeństwo naszych kont internetowych, czyli o nasze hasła. Pamiętajmy, że hasła powinny być przede wszystkim długie i unikatowe. Co to znaczy? Unikatowe hasło to takie, które jest inne dla każdej usługi, z której korzystamy. Wiem, że stworzenie wielu, a czasem nawet kilkuset różnych, długich i silnych haseł może być trudne. Dlatego warto korzystać z menedżerów haseł, które pomagają przechowywać i zarządzać nimi w bezpieczny sposób. Oprócz silnych haseł, niezwykle ważne jest również korzystanie z weryfikacji dwuetapowej, zwanej również uwierzytelnianiem dwuskładnikowym. Wiele osób już używa tego rozwiązania, nie tylko w bankowości elektronicznej, ale także podczas logowania do mediów społecznościowych czy skrzynek e-mail. Dlaczego weryfikacja dwuetapowa jest tak istotna? Ponieważ znacząco zwiększa

bezpieczeństwo naszych kont. Nawet jeśli ktoś zdobędzie nasze hasło, weryfikacja dwuetapowa stanowi dodatkową barierę, która może skutecznie zapobiec nieautoryzowanemu dostępowi.

Weryfikacja dwuetapowa skutecznie chroni nasze dane oraz dostęp do nich. Polega ona na logowaniu do zasobów za pomocą dwóch składników. Pierwszym składnikiem jest najczęściej hasło ustalone przez użytkownika, a drugim dodatkowy element, taki jak token z aplikacji, kod SMS wysyłany na telefon lub kod przesyłany na adres e-mail. Oprócz dbania o silne hasła i korzystania z weryfikacji dwuetapowej, ważne jest także odpowiednie zarządzanie dostępami do usług, zwłaszcza w kontekście organizacji. Pamiętajmy, że nie każdy pracownik powinien mieć dostęp do wszystkich zasobów. Dostępy powinny być przyznawane w sposób przemyślany, tak aby pracownicy mieli dostęp wyłącznie do tych narzędzi i usług, które są im niezbędne do wykonywania obowiązków. Dzięki takiemu podejściu znacząco zwiększamy bezpieczeństwo organizacji. Warto również zwrócić uwagę na rozdzielanie spraw prywatnych od służbowych. To dotyczy nie tylko cyberbezpieczeństwa, ale także równowagi między pracą a życiem prywatnym (work-life balance). Po zakończeniu pracy pamiętajmy o tym, aby zadbać o czas dla siebie i bliskich, co jest równie istotne jak bezpieczeństwo w sieci.

Natomiast gdy mówimy o cyberbezpieczeństwie, pamiętajmy, abyśmy zawsze sprawy służbowe załatwiali na naszym sprzęcie służbowym, natomiast sprawy prywatne na sprzęcie prywatnym. Wiem, że może to być trudne i wiem, że zapewnienie kilku, być może kilkunastu urządzeń, które by pozwalały na taki dostęp może być trudne, Ale z pomocą przychodzi nam tutaj możliwość tworzenia wielu kont na różnych, na różnych urządzeniach. Co to znaczy? Jeśli z naszego laptopa korzystamy zarówno w celach prywatnych, jak i zawodowych, warto rozważyć założenie sobie dwóch kont. Jedno konto, z którego będziemy korzystać do spraw służbowych, natomiast drugie konto do tego, gdzie będziemy korzystać ze spraw prywatnych. To samo, kiedy z urządzenia korzysta kilku użytkowników. Załóżmy dla każdego użytkownika osobne konto. Dzięki temu zwiększamy bezpieczeństwo naszej organizacji i dzięki temu istnieje mniejsze ryzyko, że gdzieś nasze dane wycieką. Jeśli pracownik będzie załatwiał swoje sprawy prywatne i na przykład kliknie w wiadomość o nieopłaconej fakturze na jego prywatnym koncie, nie zainfekuje urządzenia służbowego. Niezwykle ważne jest to, aby w organizacji jasno określić zasady korzystania z różnych urządzeń. Wiem, że w wielu organizacjach, wielu firmach pracownicy korzystają również ze sprzętu prywatnego do spraw służbowych i uzyskują dostęp do danych firmowych z różnego miejsca w różnym czasie.

Zadbajmy o to, aby w naszej organizacji wprowadzić jasne zasady dotyczące logowania – określające, kiedy i w jaki sposób pracownik może uzyskiwać dostęp do systemów. Ważne jest także monitorowanie i kontrolowanie aktywności pracowników, aby zapobiec nieuprawnionemu dostępowi do danych. Kolejnym kluczowym elementem bezpieczeństwa jest regularne aktualizowanie oprogramowania oraz urządzeń. Dlaczego jest to takie ważne? Nieaktualizowane systemy i sprzęty są bardziej podatne na różnego rodzaju ataki i zagrożenia. Regularne wprowadzanie aktualizacji może nie tylko uchronić nas przed cyberatakami, ale również mieć znaczenie wizerunkowe – świadczy o profesjonalnym podejściu organizacji do bezpieczeństwa. Niestety, zdarza się, że aktualizacje odkładamy na później, co może prowadzić do nieprzyjemnych sytuacji. Wyobraźmy sobie, że podczas ważnego spotkania biznesowego lub w trakcie wykonywania istotnych zadań nasze urządzenie nagle wymusza aktualizację i się restartuje. To nie tylko zakłóca pracę, ale może również wpłynąć negatywnie na naszą efektywność. Dlatego warto pamiętać, aby instalować aktualizacje od razu po otrzymaniu powiadomienia o ich dostępności. Odkładanie ich na później zwiększa ryzyko problemów i może prowadzić do nieprzewidzianych komplikacji. Regularne aktualizacje to prosty, ale niezwykle skuteczny sposób na ochronę naszej organizacji przed cyberzagrożeniami.

Gdy mówimy o cyber higienie. Niezwykle ważne jest to, aby zadbać o bezpieczeństwo danych, które przesyłamy w naszej organizacji. Dlaczego? Bo gdy tego nie wprowadzimy, nasze dane mogą trafić w niepowołane ręce i niestety w różny sposób mogą być wykorzystane. W jaki sposób zadbać o bezpieczeństwo przesyłania danych? Są różne rozwiązania. Niezwykle ważne jest to, aby rozważyć korzystanie z szyfrowanych sieci czy z różnych narzędzi, które umożliwiają dostęp do naszych danych firmowych, na przykład poprzez logowanie czy podwójną weryfikację. Żeby chronić to, co przetwarzamy w naszej organizacji, gdy decydujemy się na wprowadzenie Różnych narzędzi do komunikacji, z których korzystają nasi pracownicy czy my sami. Warto wybrać takie narzędzia, które rzeczywiście będą chroniły bezpieczeństwo naszych wiadomości i bezpieczeństwo naszych danych. To, jakie narzędzia Państwo wybierzecie zależy tylko i wyłącznie od Was. Ale gdy będziecie przeglądać różnego rodzaju oferty, poszukajcie takich rozwiązań, które na przykład będą gwarantowały szyfrowanie end to end. Co to jest? Jest to takie szyfrowanie przesyłanych informacji, dzięki któremu widzą je tylko osoba wysyła wysyłająca wiadomość i osoba odbierająca wiadomość. Nikt pomiędzy.

Wiadomości pomiędzy są zaszyfrowane i takie wiadomości nie wpadają w niepowołane ręce. Gdy mówimy o bezpieczeństwie przesyłania danych, pamiętajmy też o samym szyfrowaniu

danych. Myślę, że wielu z Państwa korzysta z różnego rodzaju nośników zewnętrznych, z różnego rodzaju rozwiązań pamięci przenośnej. I być może nie wszyscy pamiętacie o tym, aby wszystkie takie dane szyfrować. Pamiętajmy, aby nasze urządzenia czy to komputery, telefony, ale także pendrive'y, dyski przenośne były szyfrowane. Szyfrujmy je za pomocą silnych haseł. Szyfrujmy je za pomocą różnych narzędzi, bo jeśli wpadną one w niepowołane ręce, może to uchronić przed tym, że osoby trzecie otrzymają dostęp do naszych danych. Gdy mówimy o nośnikach zewnętrznych, bardzo ważne jest również to, aby wprowadzić w firmie w swojej organizacji procedury, które jasno będą określały, z jakich nośników mogą pracownicy korzystać oraz w jaki sposób z nich korzystać. Niestety często się zdarza, że osoby, które znajdą pendrive, dysk przenośny czy jakiekolwiek inne urządzenie gdzieś tam z ciekawości próbują sprawdzić co ono zawiera. I z pozoru może to być ludzka ciekawość i z pozoru może to być bezpieczne.

Jak się okazuje, zewnętrzne nośniki danych, których pochodzenia ani zawartości nie jesteśmy pewni, mogą stanowić poważne zagrożenie dla naszej organizacji. Takie nośniki mogą zawierać szkodliwe oprogramowanie, które może zainfekować nasze urządzenia lub sieci, co w konsekwencji może mieć poważne skutki dla działalności firmy. Gdy mówimy o nośnikach zewnętrznych, warto poruszyć również temat kopii zapasowych danych. Kopie zapasowe są jednym z najskuteczniejszych narzędzi ochrony firmy przed utratą danych. Stanowią one kopie kluczowych informacji przechowywanych w organizacji lub prywatnie. Niestety, wiele firm i pracowników zapomina o regularnym tworzeniu kopii zapasowych, mimo że są one niezwykle ważne. Dzięki kopiom zapasowym organizacja może zapewnić ciągłość pracy nawet w przypadku ataku typu ransomware. Niestety, brak takich zabezpieczeń często prowadzi do sytuacji, w których firmy muszą płacić okup lub ponosić ogromne straty finansowe, aby odzyskać dane i przywrócić funkcjonowanie systemów. Warto pamiętać o zasadzie 3-2-1 przy tworzeniu kopii zapasowych.

Zasada 3-2-1 określa, ile kopii zapasowych należy zrobić i jak je przechowywać. Przede wszystkim pamiętajmy: tworzymy 3 różne kopie zapasowe naszych danych. Przechowujemy je na co najmniej dwóch różnych nośnikach, z czego jedna kopia powinna znajdować się poza naszą organizacją. Dlaczego? Ponieważ w przypadku zdarzeń losowych, takich jak pożar, włamanie czy inna awaria, posiadanie wszystkich kopii zapasowych w jednym miejscu, np. na laptopie lub dysku przenośnym w miejscu pracy, może skutkować utratą wszystkich danych.

Zasada 3-2-1 jest prosta i warto ją stosować zarówno w życiu prywatnym, jak i zawodowym. Tworzenie kopii zapasowych to jedno z najlepszych narzędzi, które pomaga zapewnić ciągłość działania organizacji oraz ochronić ważne dane przed utratą.
Dbanie o cyberbezpieczeństwo i cyberświadomość w organizacji to przede wszystkim działania edukacyjne. Mogą to być różnego rodzaju akcje uświadamiające, które można przeprowadzać wewnątrz organizacji, materiały edukacyjne, z których warto korzystać, webinary, takie jak dzisiejszy, a także symulacje i ćwiczenia. Regularne podejmowanie takich działań znacząco zwiększa bezpieczeństwo danych i świadomość pracowników.

Jak takie ćwiczenia i symulacje wyglądają? Mogą to być na przykład symulacje ataku phishingowego. Dzięki temu będziemy mogli sprawdzić, czy rzeczywiście nasi pracownicy radzą sobie z mailami phishingowymi, czy coś nie działa w naszej instytucji i coś powinniśmy zmienić. Pamiętajmy, że człowiek jest najczęstszym celem ataków, a to od nas jako od pracodawców najbardziej wszystko zależy. Jeśli pracownik popełni błąd, nie powinniśmy go karać. Pamiętajmy, że prawdopodobnie jest to wina nas jako pracodawców, bo to my nie dostarczyliśmy mu odpowiednich narzędzi i to my nie zadbaliśmy o to, aby potrafił sobie radzić w tego typu sytuacjach. Starajmy się wysyłać naszych pracowników na różnego rodzaju szkolenia. O tym też już Państwu opowiadałam, ale korzystajmy też z różnego rodzaju dostępnych materiałów w sieci, które są darmowe, a które mogą być bardzo korzystne. Zachęcam do odwiedzenia takich stron internetowych jak Bezpieczny.pl. Jest to strona projektu Europejski Miesiąc Cyberbezpieczeństwa. Możecie Państwo znaleźć tam szereg różnych materiałów edukacyjnych, które mogą być pomocne dla Was samych, ale również dla Waszych pracowników. Zachęcam do śledzenia strony zespołu CERT Polska, gdzie możecie otrzymać nie tylko wskazówki i nie tylko cenne materiały edukacyjne, ale również zgłosić incydent bezpieczeństwa, jeżeli byście doświadczyli go w swojej organizacji.

Zachęcam do śledzenia materiałów na stronie Gov Polska. Możecie tam znaleźć różne materiały. Możecie znaleźć informacje o różnego rodzaju szkoleniach, które są skierowane do pracowników, do użytkowników Internetu i bardzo często są to szkolenia bezpłatne. Zachęcam również do odwiedzenia stron takich jak cisa.gov. Możecie tam znaleźć wiele różnych materiałów, które mogą być pomocne dla Was, które mogą Wam pomóc stworzyć różnego rodzaju Procedury i różnego rodzaju rozwiązania, które mogą być pomocne w Waszej firmie, a także do odwiedzenia strony projektu. Firma bezpieczna cyfrowo, ale więcej na temat tego projektu będzie opowiadał jeszcze kolega. Z mojej strony to wszystko i jeśliby się pojawiły pytania z sali, jestem gotowa odpowiedzieć.

red. Natalia Kieszek

Pani Anno, dziękujemy bardzo za prezentację. Myślę, że poznaliśmy naprawdę tutaj wiele cyberzagrożeń, które na nas czyhają, ale też wiemy już teraz jak dbać o cyber higienę. A teraz oddam głos Panu Piotrowi i myślę, że dowiemy się więcej o tym, jak firma powinna wyglądać bezpiecznie, cyfrowo.

Piotr Ławniczek

Dziękuję bardzo. Miło mi, że będę mógł dzisiaj Państwu opowiedzieć o wielu aspektach, które będą teraz już wykraczały poza elementy związane z cyber higieną, z taką podstawą, o której powiedziała Ania. To są aspekty bardzo ważne, dlatego że dotyczą każdego z nas indywidualnie, ale tak naprawdę każdej organizacji, niezależnie od tego, jakiej jest wielkości. To, o czym ja będę mówił, to też będą aspekty, które dotyczą małych i średnich przedsiębiorstw, bo tak dzisiaj adresujemy naszą prezentację. Natomiast pojęcie małe i średnie przedsiębiorstwo to jednak jest bardzo szeroki przekrój organizacji o bardzo różnej charakterystyce, szczególnie jeśli chodzi o sposób podejścia do zapewnienia bezpieczeństwa cyfrowego. Wiemy, że najmniejsze organizacje, mikro firmy, organizacje, w których pracuje 1 do 5 osób, często w takich organizacjach nie ma złożonych procesów, otoczenie organizacji jest dość ograniczone. W związku z tym stosowanie tych zasad, o których wspominała Ania, jest być może wystarczające do tego, żeby zapewnić dobrze swoje bezpieczeństwo. Kiedy jednak organizacja rośnie, kiedy tych osób zaczyna być kilkadziesiąt, kiedy pojawiają się działy, pojawiają się procesy, pojawiają się wewnętrzne struktury organizacyjne, pojawia się też znacznie szersze otoczenie zewnętrzne.

Chciałbym zwrócić uwagę na kilka dodatkowych aspektów, o których zamierzam dziś Państwu opowiedzieć. Między innymi omówimy:

- zagrożenia, które mogą Państwa dotknąć,
- zarządzanie ryzykiem w kontekście rosnącej organizacji,
- nowe konteksty cyberzagrożeń,
- budowanie wiarygodności i certyfikacji,
- a na koniec przedstawię kilka narzędzi, które można wykorzystać do diagnozowania poziomu bezpieczeństwa oraz jego podnoszenia.

Pierwszy aspekt, na który warto zwrócić uwagę, jest szczególnie trudny. Kiedy mówimy o małych i średnich przedsiębiorstwach, zauważamy, że istnieje bardzo niewiele badań

obejmujących precyzyjnie ten segment rynku. Większość badań dotyczy całego spektrum organizacji – od najmniejszych po największe. Co więcej, to właśnie duże organizacje często dominują w tych badaniach, ponieważ łatwiej jest od nich pozyskać dane. W związku z tym stają się one bardziej przystępnym obiektem badawczym. Natomiast małe organizacje, szczególnie w kontekście cyberbezpieczeństwa i zapewnienia ciągłości działania po ataku, są znacznie bardziej wrażliwe. Zazwyczaj nie dysponują tak dużymi zasobami finansowymi jak większe przedsiębiorstwa, co sprawia, że trudniej im przetrwać atak, odbudować się po nim bez ponoszenia poważnych konsekwencji. W najgorszym przypadku może to prowadzić do zawieszenia lub nawet zakończenia działalności po cyber incydencie.
Wiemy, że takie sytuacje często się zdarzają – po cyberataku część organizacji nie jest w stanie kontynuować działalności z sukcesem. Jeśli chodzi o incydenty zarejestrowane przez CERT Polska, dotyczą one wszystkich organizacji – małych, średnich i dużych. Dynamika tych incydentów jest bardzo wysoka, co pokazuje, że bezpieczeństwo nie jest stałym stanem. Powstaje pytanie: czy stosowane zabezpieczenia rzeczywiście są w stanie uchronić nas przed tymi zagrożeniami? Liczba zgłoszonych incydentów do CERT Polska gwałtownie rośnie. W 2020 roku zgłoszono już ponad 80 tysięcy incydentów. Co ciekawe, w październiku 2024 roku liczba incydentów przekroczyła już sumę zgłoszeń z całego 2023 roku, co pokazuje, że trend wzrostowy się utrzymuje. Jeśli chodzi o strukturę tych zagrożeń, dominują te, o których wcześniej wspominała Ania. Są to phishing, różnego rodzaju oszustwa oraz malware, czyli złośliwe oprogramowanie, które w niepożądany sposób przedostaje się do organizacji.

Bardzo ciekawe badanie dotyczy tego, ile incydentów dotyka poszczególne organizacje. Szczególnie interesujący jest fakt, że coraz więcej organizacji doświadcza rocznie 30 lub więcej incydentów bezpieczeństwa. To bardzo wysoka liczba, a trend ten wyraźnie rośnie. Drugie istotne spostrzeżenie wynika z tego, że wiele organizacji wciąż nie raportuje incydentów w ogóle. To ważny aspekt, nad którym warto się zastanowić, ponieważ duże organizacje są często zobowiązane przepisami prawa lub stosowanymi normami do zgłaszania, rejestrowania i posiadania odpowiednich narzędzi do wykrywania takich incydentów. Natomiast w małych organizacjach takich narzędzi często brakuje, co sprawia, że incydenty pozostają niewykryte, niezarejestrowane lub niezgłoszone. Taka sytuacja powoduje, że statystyki dotyczące organizacji, które nie raportują żadnych incydentów, należy traktować z ograniczonym zaufaniem. Jednocześnie widać, że liczba organizacji, które nie wykrywają incydentów, systematycznie maleje. Warto zwrócić uwagę na inne ciekawe dane przedstawione przez KPMG, dotyczące źródeł cyberzagrożeń – czyli skąd dokładnie te zagrożenia trafiają do organizacji.

Z perspektywy zarządów firm najważniejszą cechą zmian w obszarze cyberzagrożeń jest rosnąca aktywność zorganizowanych grup przestępczych oraz coraz większa złożoność ataków. Często grupy te są wspierane przez obce Państwa, co sprawia, że ataki mają coraz bardziej profesjonalny charakter, a obrona przed nimi staje się coraz trudniejsza. Oprócz tego nadal występują zagrożenia związane z działaniami niezadowolonych lub podkupionych pracowników, co również zauważają członkowie zarządów. Warto jednak podkreślić, że te obserwacje dotyczą w dużej mierze dużych organizacji, gdyż to one były głównym obiektem badania. Niemniej profesjonalizacja działań cyberprzestępców jest trendem, który dotyka wszystkie sektory rynku. Przejdźmy teraz do małych i średnich firm, ponieważ udało nam się dotrzeć do interesujących danych na ich temat. Jakie są cele ataków na małe i średnie organizacje? Pierwszym celem jest pozyskanie danych wrażliwych tych firm. Powody takich działań mogą być różne, o czym opowiem za chwilę. Kolejnym charakterystycznym elementem, szczególnie w kontekście startupów, jest kradzież pomysłów na biznes oraz unikalnych rozwiązań, które nie są jeszcze objęte ochroną patentową. Startupy, ze względu na innowacyjność i brak odpowiednich zabezpieczeń, często stają się łatwym celem ataków.

Na przykład to jest atak na własność intelektualną, czyli pozyskanie tej unikalnej, unikalnego czynnika konkurencyjnego, który drzemie w takich organizacjach. Kolejny element to jest próba zaburzenia ciągłości działania i jakby powód. Powody są bardzo różne tego, tego, tego zaburzenia ciągłości działania, ale to łącznie z pozyskaniem danych wrażliwych, bo służy często naruszeniu zaufania, czyli de facto swego rodzaju brudnej konkurencji. W efekcie, bo nie dość, że organizacja musi się walczyć z efektami, z efektami takiego ataku, to jeszcze musi oczywiście ogarnąć element, który jest związany z nadszarpnięciem reputacji, jeśli ten atak jest skuteczny, no i bardzo często to jest to jest ta, to jest ten element, który najtrudniej odbudować. Co więcej, jeśli dojdzie do incydentu, jeśli dojdzie do incydentu, który chociażby dotyczy ochrony danych osobowych, to oczywiście atakowany może ponieść dodatkowe konsekwencje związane z potencjalnymi karami związanymi z naruszeniem. Naruszeniem praw osób, których dane dotyczą. Ale jakie powody są. Że właśnie małe i średnie organizacje są atakowane? Bardzo często jest to oczywiście prosta kwestia ograniczone zasoby, czyli brak odpowiedniej ilości wykwalifikowanego personelu, który by dbał o cyberbezpieczeństwo i mechanizmów ochrony bezpieczeństwa.

Pozyskiwanie danych ma wiele aspektów. Jednym z nich jest wykorzystanie takich danych jako bramy do większych celów. Dotyczy to szczególnie sytuacji, gdy małe i średnie

przedsiębiorstwo współpracuje z dużymi organizacjami, będąc częścią ich łańcucha dostaw. Duże firmy często chronią swoją infrastrukturę w sposób bardzo profesjonalny, jednak cyberprzestępcy potrafią znaleźć słabsze ogniwa, czyli mniejsze podmioty, które są gorzej zabezpieczone, ale powiązane z dużymi organizacjami relacjami biznesowymi. Te słabiej chronione firmy stają się pośrednim celem, umożliwiając atakującym dostęp do infrastruktury większego podmiotu. Warto podkreślić, że takie działania opierają się na zaufaniu i ograniczonych możliwościach cyberochrony w relacjach między mniejszym a większym przedsiębiorstwem. To bardzo istotny, choć rzadko omawiany problem, który jednak odczuwają duże organizacje. Zdarza się, że właśnie za pośrednictwem ich kooperantów cyberprzestępcy próbują dostać się do głównej infrastruktury. Ostatnim ważnym elementem jest kwestia niższej świadomości personelu w małych i średnich organizacjach. Wynika to nie tylko z braku zasobów czy wiedzy, ale także z tego, że duże organizacje często są zobligowane do przestrzegania przepisów prawa, standardów i norm. Takie wymogi nakładają na nie obowiązek prowadzenia działań związanych z budowaniem świadomości w zakresie cyberbezpieczeństwa i cyberhigieny wśród pracowników. Małe firmy, które nie podlegają takim regulacjom, rzadziej inwestują w tego typu inicjatywy, co zwiększa ich podatność na ataki.

Priorytety bezpieczeństwa są kluczowym zagadnieniem. Ważne jest, aby nie powstało wrażenie, że bezpieczeństwo należy budować za wszelką cenę i maksymalnie zabezpieczać wszystko. Zawsze trzeba zadać sobie pytanie, czy organizacja dysponuje wystarczającymi środkami na takie działania. Bezpieczeństwo powinno przede wszystkim wspierać realizację celów biznesowych i być opłacalne. Warto jednak zwrócić uwagę na pewien istotny wyjątek – jeżeli Państwa organizacja podlega regulacjom prawnym lub normom, które wymagają wdrożenia określonych elementów cyberbezpieczeństwa, to kwestia opłacalności staje się sprawą drugorzędną. W takich przypadkach spełnienie obowiązujących przepisów ma pierwszeństwo. Dla większości organizacji kluczowe jest jednak określenie priorytetów: co należy zabezpieczać w pierwszej kolejności i w jakim zakresie. Chodzi o ochronę tych obszarów, które są kluczowe dla funkcjonowania organizacji i które przynoszą realne korzyści z punktu widzenia jej działalności. Cyberbezpieczeństwo powinno być integralnym elementem biznesplanu.

Chciałbym omówić kilka wspólnych elementów, które są istotne dla każdej organizacji, w tym:

- aspekty budowania systemu cyberbezpieczeństwa,
- nowe podejście do bezpieczeństwa wynikające nie tylko z Państwa działalności,
- ale również z funkcjonowania organizacji w szerszym ekosystemie dostawców, klientów oraz otoczenia prawnego.

Oczywiście każdy z Państwa wie, że to, co powinno podlegać Państwa ochronie, to jest Państwa kluczowa usługa, przewaga konkurencyjna i produkty, które są istotą Państwa działania i Państwa istnienia. Oczywiście warto zweryfikować, czy nie są nakładane na Państwa dodatkowe wymagania i oczekiwania, jeśli chodzi o otoczenie prawne. Na pewno większość Państwa dotyczy RODO. W związku z tym i Wy już wiecie, że trzeba stosować tą ochronę nie tylko po to, żeby chronić dane, ale żeby też uchronić biznes przed potencjalnymi skutkami negatywnych efektów ataku na dane osobowe. W związku z tym to jest element otoczenia, który trzeba uwzględnić przy identyfikacji stron zainteresowanych i oczekiwań, wobec tego, w jaki sposób powinniście ochronę w swojej organizacji prowadzić. Oczywiście najważniejszy element tej układanki to są Wasi klienci, ale dobrze wiedzieć, jakie są ich oczekiwania. Być może wasi klienci to jest grupa niejednorodna i jedni mają inne wymagania, inni inne. Powinniście podjąć świadomą decyzję, jakie elementy ochrony powinniście stosować w ramach właśnie ze względu na wymagania klientów i w tym momencie decydujecie, które wymagania, których klientów uwzględniacie w swojej działalności.

Oczywiście istnieje również aspekt dostawców z perspektywy dużych organizacji. W takich przypadkach dostawcy zazwyczaj muszą dostosować się do wymagań większych partnerów. Natomiast w przypadku mniejszych organizacji warto uwzględnić również wymagania dostawców i strukturę ich działania, aby skutecznie budować własny system bezpieczeństwa.
Kolejnym kluczowym elementem jest identyfikacja kluczowych aktywów, czyli tych elementów, które umożliwiają świadczenie Państwa usług. To niezwykle istotne, aby odpowiedzieć sobie na pytania:

- Jakie elementy w organizacji są kluczowe do prowadzenia podstawowej działalności?
- Jakie zasoby są niezbędne do utrzymania relacji z klientami?
- Jakie procesy u dostawców mają znaczenie dla zapewnienia ciągłości świadczenia usług w sposób niezakłócony i zgodny z wymaganiami klientów?

Na to wszystko nakłada się otoczenie prawne, które również definiuje swoje wymagania dotyczące sposobu działania organizacji. Dotychczas ten model funkcjonował stosunkowo stabilnie. Jednak od około roku sytuacja zaczyna się zmieniać, szczególnie w kontekście organizacji, które rosną i obsługują klientów będących istotnym elementem systemów takich jak krajowy system cyberbezpieczeństwa lub system finansowy.

Okazuje się, że wymagania, które klienci nakładają na Państwa organizację, mogą być rozszerzone o wymagania prawne narzucane na tychże klientów. Kluczowe hasło, które od

dłuższego czasu funkcjonuje w kontekście zmian podejścia do bezpieczeństwa, to zabezpieczenie łańcucha dostaw. Idea ta zyskała na znaczeniu w wyniku globalnych wydarzeń, takich jak pandemia czy incydent z zablokowaniem Kanału Sueskiego przez jeden statek, który wpłynął na funkcjonowanie większości przemysłu na świecie. Obecnie te wymagania, szczególnie w obszarze cyberbezpieczeństwa, skupiają się na kompleksowym spojrzeniu na łańcuch dostaw oraz zabezpieczenie usług. Dotyczy to przede wszystkim największych organizacji lub tych, które mają kluczowe znaczenie dla systemów cyberbezpieczeństwa bądź finansowych. Niemniej jednak, jeśli Państwa firma jest dostawcą dla takich podmiotów, warto zwrócić uwagę na te wymagania, ponieważ są one również przenoszone na dostawców. Obecnie te kluczowe organizacje otrzymują zestawy wymagań, które muszą spełnić, a jednocześnie są zobligowane do weryfikacji, czy ich dostawcy również spełniają te standardy. To istotny element, którym warto się zainteresować, aby pozostać konkurencyjnym na rynku. Jakie działania należy podjąć, aby spełnić te wymagania? To pytanie powinno stać się punktem wyjścia do analizy i wdrożenia działań, które umożliwią Państwa organizacji dostosowanie się do oczekiwań kluczowych klientów oraz obowiązujących przepisów.

Czasami to nie jest tylko tak, że wy funkcjonujecie bezpośrednio jako dostawcy takich podmiotów, ale może to mieć wpływ również na was jako Pod dostawców tych podmiotów. No i w związku z tym, żebyście wy mogli spełnić te dodatkowe wymagania, warto, żebyście je uwzględnili także w momencie, kiedy będziecie analizować, czy wasi dostawcy spełniają parametry usług, które wy musicie zapewnić. Dla waszych klientów Robi się taki łańcuch dostaw i łańcuch wymagań. W związku z tym identyfikacja tych oczekiwań jest kluczowa do tego, żebyście mogli prowadzić biznes w sposób bezpieczny i żebyście mogli spełnić wymagania, które kiedyś nie były wymaganiami. Tak oczywistymi, a teraz stają się takimi i stają się w kontekście i. I z mocy. Z mocy przepisów prawa. No więc dochodzimy do elementu zarządzania ryzykiem. My mamy bardzo mało czasu na to, żeby opowiadać tutaj dzisiaj państwu o tym, o tych elementach. Natomiast bardzo ważne jest to, żebyście państwo, analizując całe swoje miejsce w tym ekosystemie, klienci, dostawcy, otoczenie prawne potrafili zbudować takie elementy bezpieczeństwa, które wcale nie muszą wynikać z tego, że to jest państwa potrzeba, ale wynikają także z tego, że to są wymagania, które idą, przychodzą do państwa organizacji z zewnątrz.

I musicie nimi zarządzić. I nadal zarządzanie ryzykiem to jest element procesu biznesowego. Czyli wy musicie się zastanowić, jakiego typu obszary wymagają zabezpieczeń, w jaki sposób je zabezpieczycie. I taką analizę ryzyka warto sobie zrobić. Natomiast oczywiście

przygotowanie wszystkich zabezpieczeń dla wszystkich obszarów to jest czasami demagogia. Natomiast Państwo musicie wybrać kluczowe produkty, kluczowe procesy i aktywa, które powinny być zabezpieczone, i podjąć decyzje. To jest nadal decyzja biznesowa o tym, które obszary w jaki sposób zabezpieczyć. Jest coś takiego jak apetyt na ryzyko, co szczególnie jest istotne w małych i średnich przedsiębiorstwach, bo Państwo podejmujecie decyzję, w jaki sposób budować swoją przewagę konkurencyjną, właśnie często na bazie podejmowania ryzyka większego niż Wasi konkurenci. W związku z tym tutaj chodzi o takie świadome podejście do tego, jakie ryzyko Państwo podejmujecie i jakie są tego konsekwencje. Więc kluczowym elementem tutaj będzie podejmowanie decyzji na podstawie najlepszych informacji. Stąd taka analiza bardzo często jest potrzebna. Na pewno jest potrzebna w większych organizacjach, w mniejszych organizacjach być może macie Państwo to intuicyjnie i w głowie, i jesteście w stanie to po prostu przeprowadzić bez uruchamiania specjalnego procesu

No i już w momencie, kiedy Państwo zdecydujecie się na to, jakie zabezpieczenia wdrażacie i jakie cele dzięki temu realizujecie, warto pamiętać, że – tak jak wspomniała moja przedmówczyni – krajobraz cyberzagrożeń stale się zmienia. Wdrażając zabezpieczenia, powinniście mieć plan na to, jak utrzymywać ich skuteczność, czyli jak dostosowywać je do nowych zagrożeń i zmian. To jest szczególnie istotne, ponieważ wdrożenie zabezpieczenia kosztuje bardzo dużo, a jego doskonalenie kosztuje jeszcze więcej. Jeśli nie doskonalicie zabezpieczeń, możecie mieć przeświadczenie, że nadal są skuteczne, ale rzeczywistość może wyglądać inaczej. Brak doskonalenia może również oznaczać, że po pewnym czasie trzeba będzie wdrożyć całkowicie nowe rozwiązania od podstaw. Zgodnie z najlepszymi praktykami okazuje się, że podejście ewaluacyjne, czyli stopniowe doskonalenie, jest bardziej optymalne kosztowo niż skokowe zmiany w zakresie zabezpieczeń. Co więcej, z punktu widzenia bezpieczeństwa organizacji, jest to także podejście bardziej skuteczne. No dobrze, skoro już powiedzieliśmy sobie, że o cyberbezpieczeństwo trzeba zadbać i wdrożyć pewne elementy zabezpieczające, to oczywiście wiąże się to z poniesieniem określonych kosztów.

Ale jeśli już działacie w sposób bezpieczny, to warto skorzystać z tego jako przewagi konkurencyjnej i uwiarygodnić się przed partnerami biznesowymi. To jest element, który będzie, jest i będzie coraz bardziej istotny z punktu widzenia właśnie podejmowania decyzji o współpracy organizacji, żeby. Żebyście wy jako element takiego ekosystemu biznesowego nie obniżali poziomu bezpieczeństwa Waszych klientów. Jednym z takich obiektywnych wskaźników pokazujących, że spełniacie pewne wymagania, że dbacie o bezpieczeństwo, że dbacie w sposób ciągły o bezpieczeństwo, to jest certyfikacja. Jest wiele programów certyfikacji

na świecie, tutaj wymienionych jest dosłownie kilka tych takich, które są najbardziej popularne, jeśli chodzi o pokazanie, że jakiś element cyberbezpieczeństwa jest z państwa stosowany, jest stosowany systemowo, czyli że rzeczywiście to bezpieczeństwo nie jest realizowane ad hoc. Przykładem tu mogą być normy ISO, program Cyber Essentials w Wielkiej Brytanii i z NiST. To jest taki standard amerykański. Niestety tak się składa, że jeśli chodzi o Europę, jeśli chodzi o Polskę w szczególności takimi najbardziej podstawowymi standardami i certyfikatami, którymi. Chwalą się organizacje jako podstawą do budowania cyberbezpieczeństwa i zaufania do swojej organizacji, to są standardy ISO 27001 i 2201 i to są standardy, które oczywiście mają tą wspólną cechę wszystkich norm ISO, że są możliwe do wdrożenia w organizacji o dowolnej wielkości.

Niemniej wdrożenie takiej normy jest przedsięwzięciem dosyć pracochłonnym, pochłaniającym duże nakłady. I rzeczywiście mniejsze organizacje raczej nie decydują się na wdrożenie tych norm, a co za tym idzie potwierdzenie ich bezpieczeństwa. No, nie ma takiego odwzorowania w jakimś uznanym certyfikacie, czymś, czym mogliby się po prostu pochwalić w sposób inny niż powiedzenie no to przyjdźcie, sprawdźcie, bo u nas jest bezpiecznie. Tutaj proponujemy państwu podejście do takiego tematu, który jest aktualnie w fazie pilotażu. To jest firma bezpieczna cyfrowo. Zbudowaliśmy taki program certyfikacji, można powiedzieć, lekkiej, czyli takiej, która jest przystosowana do właśnie małych organizacji. On bazuje na Cyber Essentials, jest inspirowany Cyber Essentials brytyjskim programem, ale jest zaadoptowany do rynku polskiego. Uwzględnia trochę więcej elementów i z założenia odnosi się i certyfikuje obszary. Te obszary, które są najczęstszymi obszarami, które potencjalnie wykorzystają, wykorzystują cyber przestępcy do ataku w związku, jest. W związku z tym jest zbudowany w sposób bardzo, bardzo racjonalny. Program polega na. Jest 3 etapowy. Polega na sprawdzeniu gotowości do przejścia certyfikacji, do ewentualnych planów realizacji planów dostosowujących i realizacji certyfikacji.

Macie tutaj Państwo adres strony, gdzie można szerzej zapoznać się z programem. Ten program ma cechę, która może być szczególnie istotna z Państwa punktu widzenia – pierwszym etapem certyfikacji jest bezpłatna ankieta samooceny poziomu bezpieczeństwa. To ankieta, którą możecie wypełnić, aby odpowiedzieć sobie na pytanie: czy jesteście gotowi do certyfikacji, czy jeszcze nie. Ankietę wypełniacie dla siebie. Składa się ona z 14 sekcji, a po jej wypełnieniu otrzymujecie raport online. Zachęcam, żeby po wypełnieniu ankiety pobrać ten raport i na spokojnie przejrzeć jego wyniki. Raport jest bardzo praktyczny – wszędzie tam, gdzie ewentualnie nie spełniacie wymagań, znajdziecie informacje o tym, co należy zrobić, a także szczegółowe wskazówki lub rekomendacje dotyczące działań do podjęcia. Te rekomendacje

odsyłają również do poradnika, który jest integralną częścią programu. Poradnik można przeczytać oddzielnie, ale można go również wykorzystać do stworzenia planu doskonalenia. Dzięki temu możecie na końcu dojść do sytuacji, w której wypełniacie ankietę i możecie powiedzieć: wszystkie elementy są spełnione, wszystkie wymagania mamy zrealizowane w naszej organizacji. To jest moment, w którym możecie podjąć decyzję o podpisaniu umowy z nami i przystąpieniu do certyfikacji w ramach programu.

Dodam jeszcze, że poradnik zawiera swego rodzaju słowniczek, który może być bardzo pomocny dla osób, które nie są pewne swojej wiedzy lub nie do końca rozumieją pojęcia użyte w ankiecie. Warto korzystać z tego słowniczka, aby dobrze i precyzyjnie odpowiedzieć na pytania, co pozwoli na dokładną samoocenę i ocenę tego, na jakim etapie przygotowania do certyfikacji Państwo jesteście. Sama certyfikacja polega na wypełnieniu kwestionariusza, podpisaniu umowy i przeprowadzeniu weryfikacji zapisanych w kwestionariuszu elementów. Na tej podstawie macie Państwo szansę uzyskać certyfikat, który będzie umieszczony w bazie firm bezpiecznych cyfrowo. Będziecie mogli się nim chwalić i wykorzystywać go jako potwierdzenie zgodności z wymaganiami programu. Obecnie, jak wspomniałem, jesteśmy w fazie pilotażowej, ale docelowo program będzie akredytowany. W związku z tym certyfikat będzie w pełni wiarygodnym potwierdzeniem zgodności Państwa organizacji z wymaganiami programu w zakresie cyberbezpieczeństwa. Może on być również przydatny w kontekście budowania wizerunku Państwa firmy jako organizacji bezpiecznej cyfrowo. To tyle, jeśli chodzi o certyfikację. Bardzo Państwa do tego zachęcam.

Zachęcam do przetestowania tego podejścia. Jeśli będziecie mieli Państwo jakiekolwiek uwagi dotyczące programu, serdecznie zapraszamy do kontaktu i przesyłania swoich opinii. Jesteśmy otwarci na Państwa potrzeby i sugestie, aby dalej rozwijać program w taki sposób, który będzie dla Państwa jeszcze bardziej przyjazny i użyteczny. Na koniec chciałem opowiedzieć o kilku bezpłatnych narzędziach, które mogą pomóc w podnoszeniu poziomu bezpieczeństwa w Państwa organizacji lub zwiększyć świadomość na temat jej obecnego stanu. Wspólną cechą tych narzędzi jest to, że są one dostępne za darmo i umożliwiają zdobycie unikalnej wiedzy na temat poziomu bezpieczeństwa. Choć nie zastępują one dedykowanych badań przeprowadzanych w organizacji, to mogą przynieść wiele korzyści, szczególnie w zakresie identyfikacji obszarów wymagających poprawy. Pierwsze narzędzie to Artemis – jest to narzędzie służące do skanowania stron internetowych w celu wykrycia podatności i błędów konfiguracyjnych. Artemis jest wykorzystywany przez CERT Polska do skanowania podmiotów publicznych, ale jego funkcjonalności mogą być przydatne także dla Państwa organizacji.

Jeśli chcieliby Państwo dołączyć do takiego skanowania, należy się zarejestrować. Adres znajduje się na slajdzie. Po rejestracji otrzymacie Państwo raport z przeprowadzonego skanowania, który zawiera informacje o tym, co działa poprawnie oraz które obszary wymagają poprawy. Jest to bardzo przydatne narzędzie, które pozwala ocenić, jak bezpieczna jest Wasza strona internetowa. Kolejnym narzędziem, również wypracowanym przez CERT Polska, jest bezpieczna poczta Cert.pl. To narzędzie umożliwia sprawdzenie konfiguracji Państwa poczty elektronicznej. Weryfikuje między innymi, czy korzystacie z mechanizmów, które zapewniają, że wiadomości wysyłane z Waszych skrzynek mailowych nie trafiają do folderu spam. Niektóre systemy pocztowe weryfikują, czy adresy e-mail są poprawnie przypisane do adresów IP lub certyfikatów. W przypadku braku takich przypisań, wiadomości mogą być domyślnie oznaczane jako spam. Wdrożenie tych mechanizmów pomoże Państwu uniknąć sytuacji, w których biznesowa korespondencja trafia do spamu klientów. Innym ciekawym, bezpłatnym narzędziem jest numer do przekazywania SMS-ów z podejrzanymi linkami. Jeśli przekażecie Państwo takiego SMS-a na wskazany numer.

Dzięki temu narzędziu dowiecie się Państwo, czy otrzymany SMS to phishing, czy też nie. Co więcej, jeśli okaże się, że jest to phishing, mechanizm ten pozwoli na zablokowanie takiego linku dla wszystkich innych użytkowników, co zmniejszy ryzyko dla potencjalnych ofiar podobnych ataków. Kolejny element to lista ostrzeżeń. Jest to lista stron uznanych przez CERT Polska za niebezpieczne. Lista ta jest regularnie i bardzo często aktualizowana. Korzystają z niej najwięksi dostawcy internetu w Polsce – jeśli Państwa organizacja korzysta z usług 4-5 największych dostawców, to te listy są już zaimplementowane w ich systemach. Natomiast w przypadku korzystania z mniejszych dostawców warto samodzielnie pobrać tę listę, zaimplementować ją do przeglądarki i korzystać z ostrzeżeń o stronach niebezpiecznych. Kolejne bezpłatne narzędzie związane z podnoszeniem poziomu bezpieczeństwa jest dedykowane firmom, które intensywnie wykorzystują swoją adresację IP i posiadają usługi dostępne w sieci. Narzędzie to pozwala na weryfikację, czy w ramach adresacji IP Państwa organizacji nie dochodzi do działań o charakterze cyberprzestępczym, takich jak ataki typu DDoS czy inne niepożądane aktywności. Dzięki temu możecie Państwo lepiej zabezpieczyć swoją infrastrukturę i zapobiec wykorzystywaniu jej w nielegalnych działaniach.

Jaka jest reputacja Państwa adresacji? Czy nie jest ta adresacja blokowana w związku z jakimiś podejrzeniami, Podejrzanymi działaniami. Państwa puli adresowej. Ostatnie narzędzie to takie już bardzo specjalistyczne repozytorium służące do weryfikacji próbek oprogramowania. Czy

ono nie jest złośliwe? Po rejestracji można z niego skorzystać również na stronach Cert.pl. Krótkie podsumowanie. Jak widzieliście Państwo, ilość i wyrafinowanie cyber zagrożeń się zwiększa i nie można być na to obojętnym. Trzeba z tym walczyć. Trzeba z tym walczyć w sposób świadomy. Czyli musicie mieć świadomość, które obszary wymagają ochrony. Musicie podejmować racjonalne decyzje biznesowe w tym zakresie, tak żeby rzeczywiście optymalizować podejście do bezpieczeństwa organizacji i realizacji celów biznesowych. Kolejny element to, że cyberbezpieczeństwo może być elementem przewagi rynkowej i warto to wykorzystać. Jeśli już Państwo zainwestujecie w to cyberbezpieczeństwo, żeby je w jakiś sposób potwierdzić w sposób obiektywny, czyli najlepiej, żeby ono było potwierdzone przez niezależne organizacje, które mogą państwu chociażby wystawić certyfikat. I certyfikacja jest najbardziej uniwersalnym narzędziem, takim potwierdzającym spełnienie wymagań z zakresu cyberbezpieczeństwa. No i na koniec oczywiście warto korzystać z niezależnych mechanizmów wspierających bezpieczeństwo w firmie.

Kilka państwu pokazałem, o kilku mówiła Ania na koniec swojej prezentacji wskazywała linki do stron. Warto rzeczywiście tam sięgać. Jest bardzo dużo materiałów pozwalających na przeszkolenie personelu i pozwalających na przetestowanie swojej infrastruktury pod kątem spełnienia wymagań bezpieczeństwa. Z mojej strony to wszystko. Dziękuję bardzo.

red. Natalia Kieszek

Panie Piotrze. Też dziękujemy za prezentację, za pokazanie narzędzi, które z których możemy korzystać bezpłatnie i myślę, że to nas najbardziej powinno zachęcić. A teraz myślę, że jeszcze czas na krótką sesję pytań i odpowiedzi. Tutaj mieliśmy na czacie taką możliwość, więc zacznę od pierwszego pytania, gdzie szukać? Od razu skieruję to pytanie do Pani Anny gdzie szukać pomocy, jeśli firma padła ofiarą ataku typu ransomware?

Anna Kwaśnik

Przede wszystkim pamiętajmy o tym, żeby nie dać się ponieść chwili i nie płacić żądanego okupu, bo tak jak już wspomniałam na swojej prezentacji, tak naprawdę nie mamy pewności czy cyberprzestępcy rzeczywiście odblokują nam nasze dane, a także to, czy te dane nie zostaną udostępnione, czy tak właściwie już nie zostały gdzieś udostępnione. Jeżeli byście się borykali z takim problemem, jeżeli rzeczywiście wasza organizacja spotka się z tego typu zagrożeniem. Pamiętajcie, żeby skorzystać z pomocy specjalistów. Niestety, prawdopodobnie nie będziecie w stanie odblokować tego typu oprogramowania. Istnieją jednak różnego rodzaju organizacje.

Jedną z takich organizacji jest Project Nomoreransom.org, gdzie możecie sprawdzić i być może uda Wam się odblokować czy znaleźć rodzinę złośliwego oprogramowania, które zna już narzędzie deszyfrujące. Oczywiście, jeślibyście doświadczyli tego typu ataku, zachęcam też do kontaktu z NASK, którzy być może będą mogli Wam pomóc i którzy Wam udzielą wsparcia przy ataku tego typu.

red. Natalia Kieszek

Dziękujemy Pani Anno. I myślę też, że drugie pytanie też będzie skierowane do Pani, bo wspominała Pani podczas swojego wystąpienia często o szkoleniach, że są one ważne i że należy je powtarzać. Więc tutaj mamy pytanie od widza jakie szkolenia dla swoich pracowników powinniśmy wybrać?

Anna Kwaśnik

Przede wszystkim, kierując się szkoleniami, warto zwrócić uwagę na to, czego one dotyczą oraz czy są zgodne z polityką naszej firmy. Może się okazać, że treści na szkoleniu niekoniecznie będą spójne z tym, co mamy w organizacji, a to może być kłopotliwe zarówno dla pracowników, jak i dla nas samych. Zachęcam jednak do poszukiwania darmowych szkoleń i rozwiązań, ponieważ warto zaczynać od podstaw. Zacznijmy od tego, jak reagować na różnego rodzaju zagrożenia i poznajmy podstawowe elementy bezpieczeństwa. Wybierając szkolenia dla pracowników, pamiętajmy, aby dopasować je do funkcji lub stanowiska, które pełnią w organizacji. Inne szkolenie będzie odpowiednie dla pracowników niższego szczebla, inne dla dyrekcji czy kadry zarządzającej, a jeszcze inne dla specjalistów czy osób zajmujących się cyberbezpieczeństwem. Dlatego warto przejrzeć szeroki wachlarz szkoleń i wybrać te, które będą najlepiej dostosowane do naszych pracowników. Dobrym pomysłem może być również przeprowadzenie ankiety lub rozmów z pracownikami, aby dowiedzieć się, jakie szkolenia będą dla nich najbardziej odpowiednie.

W zależności od tego, jak duża jest nasza organizacja, czego potrzebują, w jakich obszarach powinniśmy ich wesprzeć. I rzeczywiście takie szkolenia dla nich wybierajmy.

red. Natalia Kieszek

Świetnie, dziękujemy. A tutaj, Panie Piotrze, Pan prezentował dane a propos upadków firm po cyberataku i otrzymaliśmy tutaj takie pytanie.: Jeżeli dwie trzecie małych firm upada po

cyberataku, to czy są może znane statystyki? Ile upada cyberprzestępców po dokonaniu takiego cyberataku? Czyli w ogóle jak tutaj jest skuteczny wymiar sprawiedliwości?

Piotr Ławniczek

Odpowiedź na to pytanie nie jest łatwa, ponieważ cyberprzestępcy nie działają w tak sformalizowanych strukturach jak organizacje legalne. W związku z tym nie jest to proces, w którym likwidowana jest jakaś organizacja i nagle znika z rynku. Takie działania odbywają się w sposób ciągły. Chciałbym podkreślić, że kluczowym elementem w rozbijaniu grup cyberprzestępczych są działania związane ze zgłaszaniem incydentów. Dopiero mając odpowiednie dowody, system walki z cyberprzestępcami może podjąć skuteczne działania. Dlatego tak ważne jest zgłaszanie wszelkich incydentów. Grupy cyberprzestępcze są rozbijane, a nasze serwisy odnoszą w tej dziedzinie duże sukcesy. Jednak jak widzicie po statystykach, nadal pojawiają się nowe cyberprzestępcy, powstają nowe wektory ataków, a my wciąż jesteśmy w obronie – wymyślamy nowe metody obrony, opracowujemy techniki wykrywania cyberataków i likwidowania grup przestępczych. Chociaż grupy są likwidowane, statystyki pokazują, że liczba znanych międzynarodowych grup przestępczych, zwłaszcza tych zorganizowanych, nadal rośnie, pomimo sukcesów w walce z nimi.

red. Natalia Kieszek

To jeszcze tutaj pozwolę sobie zadać pytanie skąd możemy wiedzieć, czy nowe regulacje podnoszące wymogi bezpieczeństwa obejmą tutaj pytania od widza moich klientów.

Piotr Ławniczek

Najważniejsze są oczywiście relacje z klientami, bo to jest coś, co będziemy wiedzieli z pierwszej ręki i to jest ważny element z jednej strony, a z drugiej strony oczywiście to jest też śledzenie tego rynku, który państwa dotyczy, to jest śledzenie legislacji, projektów ustaw i innych przepisów, które się pojawiają. Z ustawami jest relatywnie łatwo, bo one mają dość długi tryb procedowania. W związku z tym tak, wchodzenie na strony, na strony sejmowe i weryfikacja, co potencjalnie jest w takim planie. Oczywiście wiele z tych przepisów wynika z bardziej ogólnych regulacji, które powstają na poziomie europejskim. Ich tryb wdrażania jest. Jakby usystematyzowany w bardzo duży sposób. W związku z tym jest czas, żeby się na to przygotować. Warto. Warto na pewno pracować z klientami w tym kontekście.

red. Natalia Kieszek

Dziękuję. Jeszcze jedno pytanie. Myślę, że wiele osób z nas dostało podejrzane linki. I tutaj właśnie widz nas zapytał. Czy samo usunięcie podejrzanego linku wystarczy?

Anna Kwaśnik

Ja tutaj się podłączę pod to, co mówił Piotr, że zachęcamy do zgłaszania tego typu linków i do zgłaszania tego typu wiadomości, bo tak naprawdę dzięki temu nie tylko możemy zablokować strony i zmniejszyć skuteczność tych ataków, ale też być może uda się dzięki temu doprowadzić do do. Do cyberprzestępców, którzy realizują, którzy przygotowują tego typu ataki.

Piotr Ławniczek

Usuniecie linku po kliknięciu w ten link już może być mało skuteczne. Tak odpowiem.

Anna Kwaśnik

Więc zgłaszajmy tak.

Piotr Ławniczek

I nie klikajmy w te linki.

red. Natalia Kieszek

Dziękujemy bardzo serdecznie widzom za wszystkie pytania. Myślę, że dzisiaj naprawdę poznaliśmy wiele narzędzi i też sposobów, jak chronić się jakby. Jak prowadzić bezpieczną firmę. Dziękuję. Naszym gościom dzisiaj przypominam też, że na koniec można wypełnić ankietę „Jak podobał Wam się webinar?”. A już teraz zapraszamy też na dwa spotkania stacjonarne, które odbędą się w Warszawie, w Centrum Przedsiębiorczości Smolna 4 i 12 grudnia. Serdecznie zapraszamy, a też po więcej szczegółów można sięgnąć na stronie www.biznes.gov.pl. Ukośnik Digital. Dziękujemy Państwu bardzo serdecznie za udział w dzisiejszym webinarze i myślę, że do zobaczenia.

Piotr Ławniczek

Dziękujemy.