Transkrypcja webinaru „**Jak zapobiegać i radzić sobie z cyberzagrożeniami - czyli firma bezpieczna cyfrowo**”, zorganizowanego 16 stycznia 2025 w ramach projektu Digital Biznes.

[01:00:04.23] - Osoba mówiąca 1

Digital Business. Zapraszam na kolejny podcast z tej serii. Nazywam się Paweł Oksanowicz, ale nie jestem w studiu sam. Już za chwilę przedstawię dwójkę ekspertów, natomiast na pewno dziś zajmiemy się firmą bezpieczną cyfrowo. Co się okazuje? Już co piąty polski pracownik padł ofiarą cyberataku w miejscu pracy, a jednocześnie tylko niewiele ponad połowa firm używa oprogramowania antywirusowego. A cyberzagrożenia dotyczą każdego i przedsiębiorcy, i pracownika, niezależnie od wielkości firmy i branży. I najsłabszym ogniwem najczęściej okazuje się Niestety, ale człowiek. Dlatego skuteczna ochrona przed zagrożeniami w sieci to nie tylko technologie. Jej podstawą jest świadomy i przeszkolony zespół i każdy jego element, Właściwie każdy pracownik i każda pracownica. Dlatego Ministerstwo Rozwoju i Technologii połączyło siły z NASK, aby zapewnić małym i średnim firmom odpowiednie narzędzia. Tak więc zapraszamy na webinar dla wszystkich, którzy chcą się czuć przygotowani jak zapobiegać i radzić sobie z cyber zagrożeniami, czyli firma bezpieczna cyfrowo i przedstawiam ekspertów to pani Anna Kwaśnik, ekspertka do spraw budowania świadomości cyberbezpieczeństwa w nas. Witam Panią oraz Pan Piotr Ławniczak ekspert ds. cyberbezpieczeństwa, również w NASK.

[01:01:22.19] - Osoba mówiąca 1

Witam serdecznie. Za chwilę zaczniemy, ale jeszcze zachęcam wszystkich obecnych po drugiej stronie do aktywnego udziału. Dziękujemy za Państwa obecność i zachęcamy do zadawania pytań, komentowania oraz dzielenia się uwagami w oknie czatu. Postaramy się odnieść do wszystkich na koniec spotkania. A teraz oddaję głos Pani Annie Kwaśnik. Zamieniamy się w słuch.

[01:01:58.09] - Osoba mówiąca 2

Dzień dobry, witam Państwa serdecznie na dzisiejszym webinarze. Podczas naszego spotkania chciałabym pokrótce przypomnieć kilka definicji związanych z cyberbezpieczeństwem. Omówię także najważniejsze liczby dotyczące pracowników i zagrożeń w cyberprzestrzeni. Przedstawię najpopularniejsze cyberpułapki, na które narażeni są zarówno pracownicy, przedsiębiorcy, jak i

codzienni użytkownicy internetu. Zajmiemy się również tematem cyberświadomości – czym jest i dlaczego warto w nią inwestować. Przypomnę także podstawowe zasady cyberhigieny.
Na początek zastanówmy się, czym jest cyberbezpieczeństwo. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, jest to odporność systemów teleinformatycznych na działania naruszające poufność, integralność, dostępność oraz autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
Podkreślę, że budowanie odporności systemów teleinformatycznych wymaga wielopoziomowego podejścia. Jest to proces, który angażuje różne szczeble organizacji. Bezpieczeństwo sieci teleinformatycznych, z których korzystamy, stanowi fundament cyberbezpieczeństwa.

[01:03:33.01] - Osoba mówiąca 2

Mówimy także o bezpieczeństwie sprzętu, urządzeń, aplikacji i oprogramowania, z których korzystamy zarówno w sprawach służbowych, jak i w życiu codziennym. Ważne są również procedury i praktyki obowiązujące w organizacji, które pomagają pracownikom wiedzieć, jak postępować, aby skutecznie zadbać o odporność naszej firmy.
Kiedy mówimy o odporności systemów teleinformatycznych i cyberbezpieczeństwie, nie możemy pominąć kwestii cyberodporności. Cyberodporność to zdolność firmy lub organizacji do radzenia sobie z cyberatakami – od przygotowania na potencjalne zagrożenia, przez reagowanie w trakcie ataku, po działania naprawcze i zapewnienie ciągłości operacyjnej po incydencie.
Aby zbudować efektywną cyberodporność, należy odpowiednio przygotować organizację. Kluczowym krokiem jest właściwie przeprowadzona analiza ryzyka, która pozwala opracować potrzebne procedury i polityki bezpieczeństwa. Dzięki niej można również zidentyfikować niezbędne narzędzia, które pomogą w zabezpieczeniu firmy na poziomie cyfrowym. Istotnym elementem są także kompetencje pracowników – ich wiedza i umiejętności w zakresie cyberbezpieczeństwa mają bezpośredni wpływ na poziom ochrony organizacji.

[01:05:07.21] - Osoba mówiąca 2

Niezwykle istotne jest wspieranie pracowników w rozwijaniu kompetencji związanych z cyberbezpieczeństwem. O tym, jak to robić, opowiem Państwu na kolejnych slajdach.
Kiedy mówimy o cyberbezpieczeństwie, cyberodporności i cyberświadomości, musimy pamiętać, że to właśnie ludzie są najczęściej narażeni na cyberataki. Jak pokazują badania przedstawione na prezentacji, aż jeden na pięciu pracowników zetknął się z cyberatakiem w swoim miejscu pracy. Co więcej, jeden na trzech zna osobę, która doświadczyła cyberataku w swojej firmie.
Kolejne dane pokazują skalę problemu i charakter zagrożeń. Przykładowo, aż 32% pracowników otrzymało alert z programu antywirusowego informujący o podejrzanej aktywności na ich urządzeniu. Z kolei 34% respondentów wskazało, że zna osobę, która padła ofiarą cyberataku, a

aż 47% pracowników otrzymało wiadomość z niebezpiecznego źródła, której nie zidentyfikowały narzędzia antyspamowe.
Warto pamiętać, że to my, jako pracownicy, jesteśmy najczęstszym celem cyberprzestępców. Cyberataki najczęściej wymierzone są właśnie w nas, dlatego kluczowe jest budowanie naszej świadomości i kompetencji w tej dziedzinie.

[01:06:55.22] - Osoba mówiąca 2

Dlaczego to ważne? Ponieważ to my, jako pracownicy, możemy przez przypadkowy błąd – otwierając podejrzaną wiadomość czy pobierając załącznik zawierający szkodliwe oprogramowanie – narazić firmę na poważne problemy. Kiedy mówimy o cyberprzestępstwach i różnego rodzaju oszustwach, na które jesteśmy narażeni zarówno jako pracownicy, jak i codzienni użytkownicy internetu, warto wspomnieć o pojęciu socjotechniki.
Socjotechnika to nic innego jak manipulacja mająca na celu wyłudzenie naszych danych lub nakłonienie nas do działań, które mogą posłużyć przestępcom do uzyskania dostępu do firmowej infrastruktury czy naszych prywatnych danych. Co ważne, cyberprzestępcy nie zawsze korzystają z zaawansowanych rozwiązań technologicznych – często bazują na naszych emocjach, presji czasu, personalizacji ataków oraz wpływie autorytetu.
Przykładem może być sytuacja, w której otrzymujemy wiadomość o rzekomym problemie z naszym kontem służbowym lub urządzeniem. W takich momentach towarzyszą nam często silne emocje, takie jak strach, lęk czy obawa przed konsekwencjami – na przykład karą ze strony przełożonego, wyłudzeniem danych lub blokadą konta.
Pamiętajmy, że świadomość takich zagrożeń i znajomość technik manipulacji to kluczowe elementy ochrony zarówno naszych danych, jak i bezpieczeństwa całej organizacji.

[01:08:33.13] - Osoba mówiąca 2

Przestępcy doskonale wiedzą, jak wykorzystać nasze emocje i presję czasu. Wiadomości e-mail, SMS-y czy inne formy komunikacji od oszustów często wymagają natychmiastowego działania, co dodatkowo ułatwia im osiągnięcie celu. Presja czasu jest jednym z głównych czynników sprzyjających cyberprzestępcom.
Warto również pamiętać, że cyberprzestępcy nie ograniczają się jedynie do masowego wysyłania wiadomości, które trafiają do milionów skrzynek. W przypadku ataków na firmy i organizacje często szczegółowo przygotowują swoje działania. Informacje, które publikujemy w sieci – na przykład na profilach firmowych w mediach społecznościowych czy zawodowych platformach – mogą zostać przez nich wykorzystane.
Cyberprzestępcy mogą dowiedzieć się, jakie pełnimy stanowisko, jakich systemów operacyjnych używamy, a nawet z jakiego oprogramowania korzystamy. Na podstawie tych danych przygotowują spersonalizowane wiadomości, które wydają się wiarygodne i przekonujące.

Niestety, takie wiadomości mogą skłonić nas do działań, na przykład kliknięcia w link czy pobrania załącznika, które prowadzą do skutecznych ataków phishingowych.
W kontekście organizacji i firm cyberprzestępcy często wykorzystują również wpływ autorytetu. Podszywają się pod osoby z wyższych szczebli organizacji lub zaufane instytucje, co dodatkowo zwiększa ich szanse na powodzenie ataku.

[01:10:00.16] - Osoba mówiąca 2

O ile kiedyś otrzymywane wiadomości często wyglądały na nieprawdziwe już na pierwszy rzut oka, o tyle dziś działania cyberprzestępców są znacznie bardziej precyzyjne. Dzięki informacjom zdobytym w internecie na temat nas lub naszej firmy, są w stanie przygotować wiadomości, które wyglądają wiarygodnie – jakby pochodziły od naszego przełożonego, księgowej czy innej osoby z zespołu.
Przykładowo, gdy otrzymujemy wiadomość od kogoś rzekomo z naszej firmy, proszącą o opłacenie faktury, pobranie załącznika czy zmianę numeru konta bankowego, często działamy w pośpiechu, pod wpływem emocji i autorytetu osoby nadawcy. Myśląc, że to nasz przełożony, podejmujemy szybkie decyzje i niestety, czasem wykonujemy działania, których oczekują od nas oszuści. W efekcie firma może paść ofiarą poważnego ataku cybernetycznego.
Warto pamiętać, że przestępcy wykorzystują różne kanały komunikacji. Najpopularniejszym są wiadomości e-mail, które trafiają zarówno na nasze skrzynki służbowe, jak i prywatne. Innym przykładem są SMS-y, które mogą pojawić się na naszym telefonie w codziennych sytuacjach. Cyberprzestępcy wykorzystują także inne sposoby, jak wiadomości w mediach społecznościowych czy komunikatory, dlatego warto zachować szczególną ostrożność w każdym przypadku.

[01:11:22.03] - Osoba mówiąca 2

Do kanałów wykorzystywanych przez cyberprzestępców należą również komunikatory, które coraz częściej są używane w organizacjach, połączenia telefoniczne oraz media społecznościowe. Przestępcy działają na wiele różnych sposobów, często bardzo dokładnie przygotowując swoje wiadomości. Wystarczy chwila nieuwagi, działanie w pośpiechu, aby nieświadomie doprowadzić do sytuacji, w której firma ponosi poważne straty.
Chciałabym pokazać Państwu kilka przykładów takich wiadomości, które mogą trafić na Wasze skrzynki SMS-owe czy e-mailowe. Być może niektóre z nich już kiedyś otrzymaliście. O ile kilka lat temu takie wiadomości często od razu wzbudzały podejrzenia, dziś są one znacznie bardziej dopracowane i mogą wyglądać niezwykle wiarygodnie.
Przykładem mogą być SMS-y informujące o rzekomych problemach z naszym kontem, zagrożeniu dla naszych danych, grożącym mandacie czy konieczności zmiany danych, aby uniknąć utraty środków finansowych. Pod presją czasu i w obawie przed konsekwencjami często

działamy pochopnie, starając się jak najszybciej rozwiązać problem. Niestety, takie reakcje mogą prowadzić do spełnienia zamierzeń cyberprzestępców.

[01:12:41.18] - Osoba mówiąca 2

Co się dzieje, gdy klikamy w linki dołączone do wiadomości SMS czy e-maili? Na pierwszy rzut oka może się wydawać, że nic groźnego – zostajemy przekierowani na stronę logowania, gdzie musimy podać swoje dane, takie jak imię, nazwisko czy hasło. Takie strony często wyglądają bardzo wiarygodnie i sprawiają wrażenie, że rzeczywiście należą do określonej instytucji.
Jak jednak rozpoznać, że strona jest fałszywa? O ile kilka lat temu fałszywe strony często zawierały błędy językowe, stylistyczne lub nieprawidłowe logotypy, dziś są one znacznie bardziej dopracowane i wyglądają niemal identycznie jak oryginały.
Najważniejszą wskazówką jest weryfikacja adresu strony internetowej. Jeśli próbujemy zalogować się na stronę instytucji, takiej jak urząd skarbowy, adres URL zawsze będzie oficjalny i zgodny z nazwą instytucji. Jeśli po kliknięciu w link zostaniemy przekierowani na stronę o innej, podejrzanej nazwie – jak widzicie Państwo na slajdzie – możemy być pewni, że jest to fałszywa witryna.
Pamiętajmy, że logowanie na takie strony może skutkować utratą naszych danych i narażeniem na cyberoszustwo. Aby uniknąć takiego ryzyka, zawsze sprawdzajmy dokładnie adres strony, na której mamy podać swoje dane, i nie działajmy pod wpływem pośpiechu.

[01:14:11.14] - Osoba mówiąca 2

Dobrym sposobem na uniknięcie tego typu oszustw jest dodanie do zakładek przeglądarki stron internetowych, z których regularnie korzystacie, takich jak serwisy urzędów, banków czy innych usługodawców. Jeśli otrzymacie wiadomość e-mail lub SMS o rzekomym problemie z kontem, zamiast klikać w link z wiadomości, wejdźcie na stronę przez wcześniej zapisaną zakładkę i zalogujcie się bezpośrednio. W ten sposób możecie sprawdzić, czy problem rzeczywiście istnieje, czy była to próba oszustwa.
To samo dotyczy wiadomości e-mail, które trafiają na nasze skrzynki. Na pierwszy rzut oka mogą one wydawać się wiarygodne, a towarzyszące emocje, takie jak strach czy niepewność, mogą skłaniać nas do szybkiego działania. W takich sytuacjach warto zachować spokój i dokładnie zweryfikować wiadomość.
Jak rozpoznać podejrzane e-maile? Przede wszystkim zawsze sprawdzajcie adres nadawcy. Na pierwszy rzut oka może się wydawać, że wiadomość pochodzi od dyrektora banku czy prezesa firmy. Jednak po kliknięciu w pole nadawcy można rozwinąć pełny adres e-mail. Jeśli widzimy tam podejrzany adres, który nie jest zgodny z oficjalnym adresem danej instytucji, jest to wyraźny sygnał, że mamy do czynienia z próbą oszustwa.

[01:15:33.24] - Osoba mówiąca 2

Tak jak widać na slajdzie, w czerwonej ramce, teoretycznym nadawcą wiadomości jest osoba z GW. Jednak po rozwinięciu adresu e-mail okazuje się, że wiadomość pochodzi od kogoś zupełnie innego, kto nie korzysta z oficjalnych domen. Taki szczegół, łatwy do przeoczenia w pośpiechu, może sprawić, że klikniemy w link i zostaniemy przekierowani na stronę internetową, na której mamy się zalogować.
Zwróćcie uwagę na adres strony – prawdopodobnie różni się od tego właściwego. Rządowe strony czy serwisy instytucji, z których korzystacie, mają zazwyczaj domenę kończącą się na gov.pl lub inną oficjalną. Jeśli adres jest inny, to wyraźny sygnał, że mamy do czynienia z oszustwem. Dlatego zachęcam do dodawania takich stron do zakładek w przeglądarce i unikania logowania się przez linki otrzymane w wiadomościach. Dzięki temu znacząco zwiększycie swoje bezpieczeństwo. W przykładzie na slajdzie możecie zauważyć również, że strona, która teoretycznie pochodzi od instytucji rządowej, nie znajduje się w domenie gov.pl, co wyraźnie wskazuje na próbę oszustwa. Kiedy mówimy o zagrożeniach dla firm i organizacji, warto także wspomnieć o oszustwach typu *Business Email Compromise* (BEC). Są to wysoce ukierunkowane ataki, w których przestępcy podszywają się pod członków organizacji lub zaufane instytucje, aby uzyskać poufne informacje, dane finansowe lub nakłonić do wykonania przelewu.

[01:17:06.08] - Osoba mówiąca 2

Oszustwa typu *Business Email Compromise* (BEC) to ataki wykorzystujące wizerunek naszego przełożonego lub innej osoby z organizacji. Jak działają cyberprzestępcy? Przede wszystkim zbierają informacje o naszej firmie i jej pracownikach, a następnie przygotowują e-mail skierowany do konkretnej osoby. Wiadomość ta do złudzenia przypomina autentyczną korespondencję. Przykładowo, taka wiadomość może rzekomo pochodzić od dyrektora, przełożonego lub księgowej, z prośbą o natychmiastowy przelew. Bardzo często zawiera także prośbę o zachowanie poufności – "nie informuj nikogo". Dlaczego? Ponieważ takie zabiegi wzmacniają wrażenie autentyczności i powodują, że pracownik czuje presję, jakby rzeczywiście wykonywał polecenie zaufanej osoby. Co się dzieje, gdy pracownik podejmie działania opisane w e-mailu? Może to oznaczać pobranie załącznika, otwarcie fałszywej faktury lub dokonanie przelewu na wskazane konto. Niestety, przelew, który miał trafić do kontrahenta czy przełożonego, w rzeczywistości zasila konto cyberprzestępców.
Co więcej, takie wiadomości często zawierają załączniki, które po otwarciu infekują urządzenie pracownika. Infekcja może rozprzestrzenić się na całą firmową sieć, prowadząc do ujawnienia poufnych informacji, ich zaszyfrowania lub kradzieży. Konsekwencje takich działań są poważne – mogą wpłynąć na wizerunek firmy, utrudnić jej działanie, a nawet całkowicie wstrzymać działalność operacyjną. Najczęściej takie ataki to ataki typu ransomware. *Ransomware* to szkodliwe oprogramowanie, którego celem jest zablokowanie dostępu do danych lub urządzeń.

Cyberprzestępcy żądają okupu w zamian za odblokowanie danych lub urządzeń. Tego typu ataki mają różny przebieg, ale schemat jest zazwyczaj podobny. Włamanie do sieci może nastąpić w wyniku otwarcia zainfekowanego pliku przez pracownika lub zaniedbania zasad bezpieczeństwa, takich jak używanie zbyt słabych haseł do systemów.

[01:20:40.24] - Osoba mówiąca 2

Gdy dojdzie do takiego rozpoznania przez cyberprzestępców, jak wygląda sieć, najczęściej dochodzi do tego, że dane zostają skopiowane. Dane zapasowe, które przechowujemy. Niestety bardzo często na tym samym urządzeniu zostają zablokowane, a na naszych urządzeniach pojawia się notka, która mówi o tym, że Twój sprzęt został zainfekowany. Jeśli chcesz odzyskać pieniądze, musisz wpłacić taką i taką sumę na wskazane konto. W jaki sposób może dojść do zainfekowania naszego urządzenia czy naszej sieci służbowej? Przede wszystkim wspomniana już przeze mnie zainfekowane pliki, ale także fałszywe, przygotowane przez cyberprzestępców stronę internetowe. Wspomniane już przeze mnie słabe hasła, ale także nieaktualizowane systemy i aplikacje, z których jak się okazuje wielu z nas dalej korzysta. Jeśli chodzi o ataki typu ransomware, są one nie tylko niebezpieczne, ale mogą przynieść ogromne straty dla naszej organizacji. Są to przede wszystkim straty finansowe, straty reputacyjne, prawne, a także straty technologiczno operacyjne, które mogą prowadzić do wstrzymania ciągłości działania naszej organizacji. Tutaj chciałabym Państwu pokazać, jak wygląda taka notka ataku typu ransomware. Jest to tylko przykład. Przeważnie taka notka zawiera informacje, na jakie konto należy wpłacić pieniądze.

[01:22:13.06] - Osoba mówiąca 2

Kiedy cyberprzestępcy zidentyfikują, jak wygląda nasza sieć, bardzo często kopiują zgromadzone dane. Co gorsza, dane zapasowe, które przechowujemy na tym samym urządzeniu, również mogą zostać zablokowane. Na ekranie naszych urządzeń pojawia się wtedy komunikat informujący, że sprzęt został zainfekowany, a aby odzyskać dostęp, należy wpłacić określoną kwotę na wskazane konto. Jak może dojść do zainfekowania urządzenia lub sieci służbowej? Przede wszystkim poprzez zainfekowane pliki, fałszywe strony internetowe przygotowane przez cyberprzestępców, a także przez wykorzystanie słabych haseł czy brak aktualizacji systemów i aplikacji, z których korzystamy. Niestety, wiele osób wciąż używa przestarzałych wersji oprogramowania, co znacząco zwiększa ryzyko ataku.
Ataki typu *ransomware* są niezwykle niebezpieczne i mogą powodować ogromne straty dla organizacji. Są to między innymi:

- **Straty finansowe** – związane z okupem i kosztami odzyskania danych.
- **Straty reputacyjne** – utrata zaufania klientów i partnerów.
- **Straty prawne** – związane z naruszeniem przepisów o ochronie danych.

- **Straty technologiczno-operacyjne** – w tym wstrzymanie ciągłości działania firmy.

Na slajdzie chciałabym Państwu pokazać przykład notki ataku typu ransomware. Taka notka zazwyczaj zawiera szczegóły dotyczące kwoty okupu oraz numeru konta, na które należy dokonać wpłaty. Pamiętajmy, że ignorowanie zasad cyberbezpieczeństwa może prowadzić do takich sytuacji i poważnie wpłynąć na funkcjonowanie organizacji.

[01:23:47.20] - Osoba mówiąca 2

Najczęściej okup w atakach typu ransomware opłacany jest za pośrednictwem kryptowalut, a firmie wyznaczany jest określony czas na dokonanie płatności w celu odzyskania danych. Pamiętajmy jednak, że nawet po opłaceniu okupu nie mamy pewności, czy nasze dane zostaną odzyskane, ani czy nie trafią w niepowołane ręce lub nie zostaną upublicznione w sieci.

Po omówieniu najważniejszych zagrożeń, na które jesteśmy narażeni jako przedsiębiorcy i pracownicy, warto zastanowić się, dlaczego budowanie świadomości cyberbezpieczeństwa jest tak istotne i jak skutecznie przeprowadzać takie działania w naszych organizacjach.

Dlaczego warto budować świadomość cyberbezpieczeństwa? Przede wszystkim dlatego, że edukacja pracowników to kluczowy element ochrony przed cyberzagrożeniami. Szkolenia z zakresu cyberbezpieczeństwa powinny:

- Odbywać się **cyklicznie**.
- Być **dostosowane do poziomu wiedzy pracowników**.
- Odbywać się **przy rozpoczęciu pracy w organizacji** oraz **po każdym incydencie bezpieczeństwa**.

Podczas szkoleń warto przypominać o zasadach **cyberhigieny** i **cyberświadomości**. Pracownicy powinni być na bieżąco z najnowszymi zagrożeniami oraz sposobami, jak im zapobiegać. Aktualna wiedza z zakresu cyberbezpieczeństwa pozwala na skuteczniejsze reagowanie na potencjalne incydenty. **Świadomość zagrożeń** to fundament bezpieczeństwa każdej organizacji. Dzięki niej pracownicy są bardziej czujni, wiedzą, jak rozpoznawać próby oszustwa, i rozumieją, jak ich działania mogą wpłynąć na całą organizację. Budowanie takiej świadomości to inwestycja w bezpieczeństwo, które chroni firmę przed stratami finansowymi, reputacyjnymi i operacyjnymi.

[01:25:11.20] - Osoba mówiąca 2

Jak tworzyć silne hasła i jak postępować w przypadku incydentów? To kluczowe pytania, które należy uwzględnić w procesie budowania świadomości cyberbezpieczeństwa. Bardzo ważne jest, aby działania związane z cyberbezpieczeństwem były ciągłe i systematyczne. Taką ciągłość może zapewnić dobrze zaplanowany i wdrożony program budowania świadomości cyberbezpieczeństwa, o którym wcześniej wspominałam. Warto rozważyć wprowadzenie takiego programu w swojej organizacji.

Ciągłe działania na rzecz bezpieczeństwa
Działania te mogą obejmować różnorodne zadania i ćwiczenia, które pozwolą regularnie sprawdzać, czy firma jest odpowiednio zabezpieczona. Zachęcam do:

- **Przeprowadzania testów bezpieczeństwa** – aby zidentyfikować ewentualne słabości systemu.
- **Ćwiczeń i symulacji** – które sprawdzą, czy pracownicy potrafią prawidłowo zareagować, np. w przypadku otrzymania podejrzanej wiadomości e-mail.

Te działania pomagają określić, co należy poprawić i jak udoskonalić procedury. Pamiętajmy, że wsparcie pracowników w tych procesach jest kluczowe, ponieważ to oni są najczęstszymi celami cyberataków. Kultura bezpieczeństwa w organizacji opiera się na promowaniu zasad cyberhigieny oraz edukacji. Pracownicy powinni wiedzieć:

- **Jak reagować na nietypowe wiadomości.**
- **Jak zgłaszać incydenty bezpieczeństwa.**
- **Jak chronić swoje hasła i dane.**

Świadomość i odpowiednie przeszkolenie pracowników to fundament skutecznej obrony przed zagrożeniami. Budowanie kultury bezpieczeństwa to inwestycja w ochronę całej organizacji przed stratami finansowymi, wizerunkowymi i operacyjnymi.

[01:26:45.22] - Osoba mówiąca 2

Dzięki temu rzeczywiście nasza organizacja będzie bardziej bezpieczna. Pamiętajmy o tym, że w razie, gdy dojdzie do incydentu, nigdy nie należy karać naszych pracowników, ponieważ to tak naprawdę wina nas samych, jako kadry zarządzającej. To my prawdopodobnie nie zadbaliśmy o naszych pracowników – nie dostarczyliśmy im odpowiednich narzędzi, wiedzy ani kompetencji, które mogłyby powstrzymać dany atak cybernetyczny. O budowaniu świadomości można by mówić przez cały jeden webinar, ale ze względu na ograniczenia czasowe chciałabym pokazać Państwu proste narzędzia, które mogą pomóc w edukacji pracowników. Wspomniane już wcześniej szkolenia są niezwykle ważne – warto wysyłać na nie pracowników oraz przeprowadzać je w organizacji. Należy także stosować różnego rodzaju działania uświadamiające, takie jak alarmowanie o nowych kampaniach phishingowych, informowanie o konieczności przeprowadzenia aktualizacji czy też o wykrytych podatnościach w urządzeniach i oprogramowaniu, z których korzystamy. Niezwykle ważne jest również, aby uzbroić pracowników w różnego rodzaju materiały edukacyjne, które pozwolą im stale podnosić swoją świadomość i wiedzę z zakresu cyberbezpieczeństwa.

[01:28:12.22] - Osoba mówiąca 2

Takich materiałów edukacyjnych można znaleźć bardzo dużo w internecie. Na sam koniec swojej prezentacji pokażę Państwu kilka stron internetowych, z których warto korzystać. Dzięki takim

materiałom Wasi pracownicy będą mogli podnosić swoje kompetencje i poszerzać swoją wiedzę. Zachęcam również do uczestnictwa w różnego rodzaju webinarach, takich jak ten dzisiejszy. To doskonała okazja, by dowiedzieć się wielu przydatnych informacji, które mogą znaleźć zastosowanie w codziennej pracy. Warto także regularnie organizować symulacje i ćwiczenia, aby sprawdzić, jak w praktyce radzą sobie nasi pracownicy, co jeszcze wymaga poprawy oraz jakie narzędzia i kompetencje powinniśmy dalej rozwijać w zespole.
Pod koniec swojej prezentacji chciałabym przypomnieć Państwu kilka podstawowych zasad cyberhigieny. Gdy mówimy o podnoszeniu świadomości cyberbezpieczeństwa, nie sposób pominąć tego tematu. Chciałabym wskazać kilka najważniejszych zasad, które, mam nadzieję, już stosujecie w swoim życiu. Jeśli jednak jeszcze ich nie wdrożyliście, to liczę, że po tym szkoleniu włączycie je do swoich codziennych praktyk. Przede wszystkim pamiętajmy, że jednym z najważniejszych elementów chroniących nasze dane, nas samych oraz całą firmę, jest przestrzeganie podstawowych zasad cyberhigieny.

[01:29:34.09] - Osoba mówiąca 2

Nasze organizacje mogą być silne i bezpieczne, jeśli będziemy stosować odpowiednie zasady ochrony. Jednym z kluczowych elementów są silne hasła. Mówiąc o silnych hasłach, mam na myśli te, które składają się z co najmniej 14 znaków. Im dłuższe hasło, tym trudniejsze do złamania. Ważne, aby hasło było unikatowe, czyli inne dla każdej usługi, z której korzystamy. Wiem, że może to wydawać się trudne do zrealizowania i budzić pewne obawy, ale pomocne w tym przypadku mogą być menedżery haseł.
Menedżery haseł to narzędzia, które nie tylko pomagają tworzyć i zapamiętywać hasła, ale także oferują dodatkowe funkcjonalności. Jedną z nich, często pomijaną, jest ochrona przed logowaniem na fałszywych stronach internetowych. Jeśli spróbujecie Państwo zalogować się na takiej stronie, menedżer haseł nie pozwoli na użycie zapisanych danych, co stanowi dodatkową warstwę ochrony. Jeśli jeszcze nie korzystacie z menedżera haseł, zachęcam do rozważenia zakupu lub skorzystania z dostępnych darmowych opcji w sieci.
Pamiętajmy również o ochronie dostępu do naszych danych i firmowych systemów. Kluczowe jest, aby zadbać o bezpieczne połączenia oraz właściwe zarządzanie dostępami pracowników do firmowych zasobów. Odpowiednie procedury i narzędzia mogą znacząco zwiększyć bezpieczeństwo organizacji.

[01:31:03.10] - Osoba mówiąca 2

Pamiętajmy, aby wprowadzić odpowiednie uprawnienia wśród pracowników, tak aby dostęp do tajnych i poufnych informacji mieli tylko ci, którzy rzeczywiście tego potrzebują. To samo dotyczy dostępu do uprawnień administratora na komputerach – warto dokładnie przeanalizować, jakie uprawnienia są niezbędne poszczególnym pracownikom, i przypisywać je w sposób przemyślany.

Zachęcam również do jasnego określenia zasad dotyczących korzystania ze sprzętu służbowego do celów prywatnych i odwrotnie. Rozdzielanie spraw prywatnych od służbowych jest niezwykle ważne, szczególnie w kontekście bezpieczeństwa. Zasada work-life balance jest tu bardzo pomocna – w pracy zajmujemy się sprawami zawodowymi, a w domu skupiamy się na prywatnych. Stosujmy te zasady również w kontekście urządzeń i skrzynek pocztowych. Dlaczego to istotne? Jeśli korzystamy z jednego komputera zarówno do spraw prywatnych, jak i służbowych, atak na prywatną skrzynkę e-mail może skutkować utratą danych lub informacji związanych z pracą.
Bardzo ważne jest również jasno określenie zasad korzystania z urządzeń prywatnych. Pracownicy powinni wiedzieć, w jakim zakresie mogą korzystać z prywatnych urządzeń do celów służbowych i odwrotnie, aby zminimalizować ryzyko naruszenia bezpieczeństwa danych organizacji.

[01:32:29.20] - Osoba mówiąca 2

Wiem, że wiele firm, wiele przedsiębiorców pozwala na to, aby pracownicy wykorzystywali swoje prywatne urządzenia do celów służbowych. Żeby one były bezpieczne. Stwórzcie odpowiednią politykę bezpieczeństwa. Zadbajcie o to, aby jasno określić, że na przykład korzystamy z jednego urządzenia, ale posiadamy dwa osobne konta na komputerze, gdzie jedno służy do celów prywatnych, a drugie służy do tych celów służbowych. Pamiętajmy również o tym, aby przeprowadzać aktualizacje. Bardzo dobrym rozwiązaniem jest włączenie automatycznych aktualizacji. Dzięki czemu Wasze urządzenia będą wymuszały na pracownikach to, aby przeprowadzić daną aktualizację. Dobrym rozwiązaniem jest to określenie dnia. Daty czy nawet godziny, do której aktualizacje należy zrobić. Jeśli pracownik nie kliknie, nie zrobi tego samodzielnie. Wówczas włączyć taką opcję, żeby sprzęty się automatycznie aktualizowały. Dzięki temu urządzenia pracowników czy to telefony, czy laptopy, czy jakiekolwiek inne, będą posiadały aktualne wersje. Dzięki czemu będą mniej podatne na różnego rodzaju luki bezpieczeństwa, będą mniej podatne na różnego rodzaju ataki. Zadbajmy również o to, aby dane, które przesyłamy w naszej organizacji, były bezpieczne. W jaki sposób?

[01:34:00.22] - Osoba mówiąca 2

Przede wszystkim warto zastanowić się, z jakich narzędzi i rozwiązań korzystamy w naszej organizacji. Zanim zdecydujemy się na wybór komunikatora, dostawcy poczty służbowej czy jakiejkolwiek innej aplikacji, konieczne jest zapoznanie się z polityką bezpieczeństwa tych usług. Sprawdźmy, jakie standardy bezpieczeństwa oferują i jakie usługi gwarantują.
Zachęcam do korzystania z komunikatorów i narzędzi, które oferują szyfrowanie wiadomości w taki sposób, aby były one widoczne wyłącznie dla nadawcy i odbiorcy. Jest to tzw. szyfrowanie end-to-end, które znacząco podnosi poziom bezpieczeństwa przesyłanych danych.

Warto również przypomnieć o polityce dotyczącej zewnętrznych nośników danych. To właśnie pendrive'y, dyski przenośne czy inne nośniki, które podłączamy do komputerów, mogą stanowić zagrożenie dla bezpieczeństwa naszej organizacji. Dlatego należy jasno określić zasady ich użytkowania i upewnić się, że pracownicy działają zgodnie z ustalonymi procedurami.
Jeśli korzystamy z zewnętrznych nośników danych, warto je szyfrować, aby chronić zawarte na nich informacje. W przypadku, gdy przekazujemy ważne dane współpracownikowi lub innym osobom za pomocą takich nośników, musimy upewnić się, że ich zawartość jest odpowiednio zabezpieczona. Takie podejście pomoże zminimalizować ryzyko naruszenia bezpieczeństwa w organizacji.

[01:35:36.02] - Osoba mówiąca 2

Pamiętajmy, aby zawsze szyfrować zewnętrzne nośniki danych silnym i bezpiecznym hasłem. Niestety takie urządzenie, jak pendrive czy dysk przenośny, może zostać zgubione lub skradzione. Jeśli osoba trzecia zdobędzie dostęp do naszych nośników, na których znajdują się poufne informacje dotyczące firmy, może wykorzystać je w niepożądany sposób. Dlatego szyfrowanie nośników i ustawianie bezpiecznych haseł to absolutna konieczność.
Zachęcam również, aby powstrzymać swoją ciekawość w sytuacjach, gdy znajdziecie Państwo na korytarzu, na zewnątrz budynku czy przy wejściu do firmy pendrive lub inny zewnętrzny nośnik. Nie podłączajcie go do swoich urządzeń, ponieważ może zawierać szkodliwe oprogramowanie. W takich sytuacjach najlepiej oddać znaleziony nośnik do działu bezpieczeństwa lub poinformować pracowników za pomocą krótkiej wiadomości e-mail. Może się okazać, że sprzęt należy do któregoś z pracowników i w ten sposób uda się znaleźć jego właściciela.
Dbanie o kopie zapasowe danych to kolejny niezwykle ważny element ochrony przed zagrożeniami. Kopie zapasowe mogą uratować firmę w przypadku ataku szkodliwego oprogramowania, takiego jak ransomware. Zawsze należy tworzyć kopie zapasowe i przechowywać je na dwóch różnych nośnikach. Przynajmniej jedna z tych kopii powinna znajdować się poza organizacją, aby zwiększyć bezpieczeństwo w przypadku awarii systemu lub ataku.

[01:37:15.09] - Osoba mówiąca 2

Dlaczego? Bo jeśli doszłoby do jakiegoś incydentu państwa firmie, gdyby doszło na przykład do chociażby pożaru, Jeśli będziecie posiadać Państwo. Wszystkie kopie zapasowe w waszym biurze w Waszej lokalizacji. Niestety, ale mogą one zostać utracone. Pamiętajmy, że dbałość o takie małe szczegóły z pozoru mogłoby się wydawać, że rzeczywiście wpływa na to, w jaki sposób nasza firma funkcjonuje, w jaki sposób nasza firma może sobie radzić z różnego rodzaju zagrożeniami i ewentualnymi cyberatakami. Tak jak wspominałam, na koniec swojej prezentacji chciałabym Państwu pokazać kilka stron internetowych, na których możecie Państwo znaleźć

materiały edukacyjne dla Was samych, ale również wykorzystać je wśród swoich pracowników. Materiały udostępniane na tych stronach są bezpłatne. Możecie z nich korzystać, Możecie je rozsyłać wśród swoich pracowników i zachęcać do tego, żeby rzeczywiście zwiększali swoją wiedzę. Zachęcam również do tego, aby śledzić strony internetowe i social media naszej organizacji, naszej instytucji, czyli NASK u. Możecie Państwo znaleźć tam bardzo dużo cennych informacji na temat bieżących zagrożeń, na temat tego, co się dzieje w świecie cyber owym, ale również w świecie technologii.

[01:38:40.07] - Osoba mówiąca 2

I z mojej strony to wszystko.

[01:38:42.03] - Osoba mówiąca 1

Bardzo dziękuję. Pani Joanna Kwaśnik NASK w prezentacji odwołała się Pani do takich życiowych spraw, jak na przykład dzielenie na jednym urządzeniu rzeczy służbowych i rzeczy prywatnych. To chyba jest duży problem w firmach. Tak mi się przynajmniej wydaje.

[01:38:56.11] - Osoba mówiąca 2

Jest to duży problem, dlatego warto wprowadzić jakieś polityki, które będą to regulowały. Bo kiedy będziemy mieszać te rzeczy rzeczywiście, gdy dojdzie do zainfekowania mojego urządzenia, bo prywatnie dostałam jakąś tam wiadomość, może to generować bardzo duże straty. Dlatego zadbajmy o to, aby rozdzielać te sprawy. I tak jak mówię, nie tylko w kontekście technologii, ale także w takim kontekście zdrowotnym.

[01:39:24.22] - Osoba mówiąca 1

Pozwoliłem sobie zadać pierwsze pytanie dzisiaj, tutaj, w naszym studiu, a tak naprawdę chciałbym w ten sposób przypomnieć państwu o tym, że jest możliwość zadawania pytań i jest możliwość komentowania wszystkiego, co się tutaj dzieje u nas w oknie czatu. Zachęcam do tego na koniec naszego dzisiejszego spotkania. Będzie taka możliwość, aby odpowiedzieć na wszystkie. Postaramy się przynajmniej odpowiedzieć na wszystkie z tych pytań. A ponieważ zapowiedziałem drugiego gościa, nie pozostaje mi nic innego, jak oddać mu głos. To pan Piotr Ławniczak, również ekspert do spraw cyberbezpieczeństwa, również reprezentujący NASK. Tak więc oddajemy panu głos.

[01:39:59.14] - Osoba mówiąca 3

Dziękuję bardzo. Chciałbym powiedzieć teraz o drugiej części zaadresowanej do państwa organizacji. Zdajemy sobie sprawę, że tak krótki webinar oczywiście nie wyczerpie wszystkich istotnych kwestii, które są w obszarze cyberbezpieczeństwa dla Państwa bardzo ważne. Z jednej strony, a z drugiej strony zdajemy sobie sprawę, że jesteście państwo bardzo różnymi organizacjami. Z jednej strony mamy i tak się spodziewam, po drugiej stronie osoby i które prowadzą jednoosobową działalność, a także organizacje, które są znacznie większe, znacznie bardziej złożone, organizacje, które także bardzo dynamicznie rosną całego sektora SME. W związku z tym to, o czym będę chciał powiedzieć Państwu w mojej prezentacji, to będzie kilka słów o zagrożeniach, które Państwu na Państwa czyhają. O tym, jak zarządzać ryzykiem. Trochę o nowym kontekście cyber zagrożeń. To w kontekście szczególnie tych firm rosnących i większych, a później o tym, o wiarygodności, o certyfikacji i o narzędziach, czyli o takich elementach, które są dla wszystkich państwa, mam nadzieję, bardzo, bardzo ważne. To, o czym mówiła moja koleżanka przed chwilą, to jest coś, co jest absolutnie uniwersalne i ważne w każdej organizacji, niezależnie od wielkości.

[01:41:26.19] - Osoba mówiąca 3

Jest bardzo mało badań, które koncentrują się na zagrożeniach skierowanych konkretnie do małych i średnich przedsiębiorstw. Niemniej jednak, takie badania się pojawiają i pokazują, że przedsiębiorstwa tego typu nie różnią się znacznie od dużych organizacji pod względem poziomu narażenia na cyberzagrożenia. Małe i średnie firmy również są celem cyberprzestępców, a liczba ataków skierowanych przeciwko nim jest podobna do tej obserwowanej w przypadku większych organizacji.
Dane CERT Polska z ostatnich lat potwierdzają, że liczba rejestrowanych incydentów rośnie gwałtownie z roku na rok. Niestety, ten rok zapowiada się jako kolejny rekordowy pod tym względem – już w październiku ubiegłego roku liczba incydentów przekroczyła całkowitą liczbę zgłoszeń odnotowanych do końca 2023 roku. CERT Polska corocznie publikuje raporty dotyczące zgłoszonych incydentów, które będą dostępne wiosną w ramach raportu rocznego.
Wśród najpopularniejszych zagrożeń rozpoznawanych przez CERT Polska wyróżniają się phishing, czyli celowane ataki na konkretne osoby i organizacje, różnego rodzaju oszustwa oraz malware, czyli złośliwe oprogramowanie. Są to dokładnie te same zagrożenia, o których wspominała moja koleżanka.

[01:43:13.08] - Osoba mówiąca 3

W przypadku zagrożeń ransomware jest jednym z najczęściej występujących problemów, z którymi organizacje muszą się mierzyć na co dzień. Jeśli chodzi o częstotliwość ataków, KPMG przygotowało zestawienie pokazujące, ile takich incydentów średnio dotyka organizacje w ciągu roku. Dane wskazują, że liczba ataków stale rośnie, a zmiany te mają dość niepokojący charakter.

Zestawienie pokazuje dolny i górny zakres liczby ataków w statystyce, co obrazuje, że ataki są coraz częstsze i łatwiejsze do przeprowadzenia. Z jednej strony wzrost wynika z coraz lepszych możliwości detekcji takich incydentów, z drugiej – z rosnącej liczby cyberataków i ich większej dostępności dla przestępców.
Jednak w tej sytuacji można zauważyć pewną lukę w danych, która wynika z faktu, że wiele firm, szczególnie małych i średnich, nie zauważa lub nie raportuje incydentów. Niestety, duża część organizacji nie posiada odpowiednich procedur lub narzędzi, które pozwoliłyby na wykrycie i zgłoszenie takich zdarzeń. To oznacza, że dane nie zawsze w pełni oddają skalę problemu. Fakt, że jedna trzecia organizacji wydaje się nie być celem ataków, może być związany z brakiem narzędzi do monitorowania i detekcji, a nie z rzeczywistym brakiem zagrożeń.

[01:44:58.22] - Osoba mówiąca 3

Jeśli chodzi o to, kto atakuje, to tutaj jest też bardzo ciekawa statystyka pokazująca, że cyberprzestępcy się profesjonalizują. To coraz mniej. Są osoby, które testują czy potrafią otworzyć jakąś stronę, dostać się w jakieś miejsce w organizacji. Coraz częściej niestety są to zorganizowane grupy przestępcze. Cyberterroryści, a także grupy wspierane przez obce państwa. Tutaj jest duża ilość informacji na ten temat na naszych stronach. Jak wyglądają tego typu ataki? Z drugiej strony mamy też świadomych, czasami nieświadomych. Cyberprzestępców de facto, którzy działają na naszą niekorzyść jako pracownicy, którzy pewne działania podejmują świadomie, intencjonalnie albo nieświadomie. I dlatego tak ważna jest cyber edukacja, o czym mówiła moja koleżanka w poprzedniej części spotkania. Dlaczego państwo jako małe i średnie przedsiębiorstwa możecie być celem ataków? Czasami to są. To jest kwestia pozyskania danych wrażliwych, które dla Was są istotne, a dla przestępcy potencjalnie albo mogą być atrakcyjne w ramach nieuczciwej konkurencji, albo mogą wywoływać chęć właśnie i szansę, że będziecie chcieli zapłacić okup za odzyskanie tych danych. Drugi element to własność intelektualna. To jest coś, co jest najważniejsze, szczególnie w startupach, gdzie ten element innowacyjności, który państwo macie, bardzo często jest elementem waszej przewagi, na którą, na której planujecie zbudować swój biznes.

[01:46:49.09] - Osoba mówiąca 3

Dlatego jest to bardzo ważna dla Was ważny element i cyberprzestępcy o tym wiedzą. Kolejny element, który też jest elementem albo takiej nieuczciwej konkurencji, albo innych celów, o których za chwilę powiem. To jest zaburzenie ciągłości działania. Relatywnie łatwo da się teraz przeprowadzić atak typu DDoS i on niestety wpływa, wpływa na organizację bądź oczywiście zaszyfrowanie danych, o których też już mówiliśmy. Też może być dla firmy dużym problemem, jeśli nie realizuje i nie przeprowadza regularnych kopii zapasowych. Oczywiście największym zagrożeniem dla państwa w kontekście tych ataków to jest to, że jeśli Państwa działanie zostanie

zaburzone, jakieś dane się wydostaną, no to to naruszenie zaufania Państwa, klientów, Państwa otoczenia biznesowego do państwa, do prowadzenia biznesu w taki sposób, w jaki Państwo to robicie. Niestety cyberprzestępcy mają świadomość i są gotowi podjąć działania, które spowodują, że te ich cele zostaną zrealizowane. Kolejnym elementem. Jakie są powody tego, że do ataków dochodzi Szczególnie małe organizacje, które szybko rosną, mają problem z tym, żeby poradzić sobie nie tylko z rozrastającymi się procesami i ilością personelu, zarządzaniem, ale także z odpowiednim dopasowaniem mechanizmów bezpieczeństwa.

[01:48:24.03] - Osoba mówiąca 3

To również jest czynnik, który cyberprzestępcy uwzględniają – łatwość dostania się do infrastruktury oraz przełamania mechanizmów cyberbezpieczeństwa. Ataki ransomware, o których wcześniej wspomniano, są tutaj szczególnie istotne. Nawet jeśli zdecydujecie się Państwo na opłacenie okupu, by odszyfrować dane, należy pamiętać, że cyberprzestępcy mogą w drugim kroku zażądać kolejnej opłaty. Tym razem będzie to opłata za to, aby dane, które zostały pobrane, nie pojawiły się na rynku i nie spowodowały incydentu bezpieczeństwa.
W kontekście regulacji, takich jak RODO, ochrona danych osobowych jest traktowana bardzo poważnie. Upublicznienie takich danych może narazić Państwa organizację na wysokie kary finansowe oraz znaczące naruszenie zaufania klientów i partnerów. Tego rodzaju incydenty mogą mieć długofalowe, negatywne skutki dla reputacji firmy.
Coraz częściej zdarza się również, że organizacje nie są bezpośrednim celem ataku, lecz stanowią bramę do większych, strategicznych celów. Jeśli współpracujecie Państwo z dużymi lub kluczowymi organizacjami, cyberprzestępcy mogą traktować Waszą firmę jako słabsze ogniwo. Duże, dobrze zabezpieczone organizacje są trudniejsze do zaatakowania, dlatego przestępcy często wybierają mniejsze firmy, które mają niższy poziom zabezpieczeń, aby dostać się do większych celów poprzez ich infrastrukturę.

[01:49:58.06] - Osoba mówiąca 3

Będą szukały najsłabszych punktów, przez które mogą się do nich dostać. Jeśli wasze cyberbezpieczeństwo nie jest na najwyższym poziomie, to być może staniecie się właśnie taką bramą wejścia do dużej organizacji poprzez to, że między wami a Waszym klientem są już nawiązane jakieś relacje zaufania i jest szansa po prostu ich wykorzystania. Zwracajcie na to uwagę. No i kolejny element to też jest kwestia tego, że organizacje, które szybko rosną, małe organizacje Nie zawsze najwyższym priorytetem dla nich jest zachowanie cyberświadomości wśród personelu personelu, który szybko przyrasta. No, tutaj trzeba też o to zadbać od początku do końca, żeby nie dawać szansy cyberprzestępcą na to, żeby żeby mieli łatwiejszy sposób do tego, żeby zaatakować. No ale kluczowym elementem bezpieczeństwa jest to, że musi służyć realizacji celów biznesowych. W związku z tym bezpieczeństwo musi się opłacać. Dlatego tak

ważne jest, żebyście państwo przy prowadzeniu swojej działalności uwzględniali element bezpieczeństwa, uwzględniali go w sposób racjonalny. Ja tutaj zrobiłem dwie gwiazdki, dlatego że coraz częściej elementy bezpieczeństwa są też wymuszane poprzez regulacje prawne i stosowanie pewnych zabezpieczeń. Po prostu wtedy wychodzi poza element biznesowy.

[01:51:24.17] - Osoba mówiąca 3

Jest po prostu elementem, który w biznesie trzeba uwzględnić jako coś, co jest wymagane. Opowiem teraz kilka słów o kluczowych aspektach budowania systemu cyberbezpieczeństwa. To będzie bardzo, bardzo skrótowe, gdyż mamy dzisiaj bardzo krótkie spotkanie, a omawianie takiego podejścia do budowania cyberbezpieczeństwa to pewnie byłby tydzień spotkań, żeby je omówić w szczegółach. Pierwszym elementem, który jest kluczowy w organizacji, szczególnie w średniej organizacji, jest dobra identyfikacja usług kluczowych, czyli tego, co jest dla Państwa największą wartością. Oczywiście to są Państwa usługi, produkty, które przynoszą największe zyski, ale także elementy państwa organizacji, które stanowią państwa przewagę konkurencyjną. Musicie zidentyfikować te elementy, bo to są elementy, które będziecie w przyszłości jak najszybciej musieli jak najlepiej chronić. Kolejne elementy to identyfikacja zainteresowanych stron i ich oczekiwań. Z jednej strony to otoczenie prawne. Każdy z Państwa ma bazę swoich klientów, już podlega pod wymagania, które wynikają z regulacji RODO, ale oczywiście tych regulacji jest znacznie więcej. Trzeba je znać, trzeba mieć świadomość ich, szczególnie, że pojawia się ich coraz więcej i te wymagania trzeba brać pod uwagę budując swój biznes, budując zabezpieczenia dla swojej organizacji.

[01:52:56.23] - Osoba mówiąca 3

Oczywiście najważniejszą stroną zainteresowaną w zakresie bezpieczeństwa są Wasi klienci. Musicie słuchać ich potrzeb i uwzględniać wymagania, które stawiają. Ważne jest, aby zapewnić ich, że wszystkie zobowiązania wynikające z podpisanych umów – szczególnie te dotyczące zabezpieczenia relacji biznesowej – zostaną dotrzymane. Podobna zasada obowiązuje w relacjach z dostawcami. W takich przypadkach również należy uwzględnić wymagania stawiane przez drugą stronę, szczególnie jeśli dostawca jest stroną dominującą, czyli większym podmiotem. To wymaga dostosowania się do określonych standardów i procedur, aby utrzymać te relacje na właściwym poziomie. Kolejnym krokiem jest identyfikacja kluczowych aktywów, które wymagają szczególnej ochrony. Należy uwzględnić przede wszystkim kluczowe usługi stanowiące przewagę konkurencyjną. Drugim istotnym aspektem są elementy, które gwarantują dostępność usługi, a więc te, które klienci uznają za absolutny standard lub które są zapisane w umowie SLA jako gwarancja jakości i dostępności produktu. Ważne jest, aby zapewnić, że te elementy będą funkcjonować bez zakłóceń, nawet w sytuacjach kryzysowych, takich jak próba

ataku cyberprzestępców. Zdolność do świadczenia usług na odpowiednim poziomie pomimo takich zagrożeń jest kluczowa dla utrzymania zaufania klientów i partnerów biznesowych.

[01:54:38.06] - Osoba mówiąca 3

Co więcej, coraz częściej otoczenie prawne nakłada na Waszych klientów, szczególnie jeśli są to duże organizacje, specyficzne wymagania w zakresie bezpieczeństwa. Przykładem mogą być dyrektywa NIS 2 czy rozporządzenie DORA, które określają standardy i obowiązki w tej dziedzinie. W praktyce oznacza to, że wymagania te będą przekładały się na oczekiwania Waszych klientów wobec Was jako ich partnerów biznesowych. To bardzo istotne, ponieważ nie są to drobne wymagania i trzeba się do nich odpowiednio przygotować. Dlatego niezwykle ważne jest śledzenie otoczenia prawnego, nie tylko związanego z Waszą działalnością, ale także z działalnością Waszych klientów. Wymagania te mogą przybierać różne formy, od konieczności poddawania się regularnym audytom przeprowadzanym przez klienta lub niezależne podmioty, po wymogi dotyczące zabezpieczeń stosowanych przez Waszych dostawców. Dotyczy to wszystkich elementów, które wykorzystujecie w świadczeniu usług na rzecz swoich klientów. Jest to bardzo złożone otoczenie, które wymaga starannego zarządzania, szczególnie jeśli rozwijacie się lub jako średnia firma współpracujecie z dużymi organizacjami. Uwzględnienie tych wymagań nie tylko zwiększa bezpieczeństwo Waszej działalności, ale także pozwala utrzymać i rozwijać współpracę z większymi podmiotami. Spełnienie tych standardów to nie tylko kwestia zgodności z regulacjami, ale również klucz do dalszego rozwoju i sukcesu na rynku.

[01:56:16.12] - Osoba mówiąca 3

W związku z tym musicie tutaj podjąć, mając te informacje wszystkie zebrane podjąć decyzję, w jaki sposób zarządzać ryzykiem. To zarządzanie ryzykiem to oczywiście podejmowanie decyzji o tym, jakie, jakie zasoby, w jaki sposób będziecie chronić, w jaki sposób zapewnicie, że ta ochrona będzie spełniała wymagania waszego otoczenia biznesowego. Wybór tych zabezpieczeń i dobra analiza są bardzo ważne, dlatego że z jednej strony musicie dobrze się zabezpieczyć, a z drugiej strony nie chodzi o to, żebyście ponieśli nadmierne koszty na te zabezpieczenia. Dlatego zderzacie potencjalne opcje możliwości zabezpieczenia z waszym apetytem na ryzyko, czyli waszą zdolnością do akceptacji pewnego ryzyka. Pamiętajcie, że to jest cecha, która jest specyficzna dla każdego z Was i każdy inaczej pewnie to określa. Dopiero zestawienie tych dwóch elementów spowoduje, że będziecie w stanie dobrać optymalne zabezpieczenia, które zapewnią odpowiednie bezpieczeństwo przy jednoczesnym zachowaniu i możliwości realizacji celów biznesowych. Także te decyzje, które będziecie podejmowali, będą wtedy optymalne, kiedy rzeczywiście weźmiecie pod uwagę całe swoje otoczenie w takiej analizie ryzyka. Oczywiście wdrożenie takich zabezpieczeń to nie jest banalna sprawa. Prawdopodobnie wiąże się z kosztami większymi bądź mniejszymi.

[01:57:48.11] - Osoba mówiąca 3

Kluczowe nie jest jednorazowe wdrożenie zabezpieczeń, ponieważ są one skuteczne jedynie w momencie implementacji. Otoczenie cyberzagrożeń stale się zmienia, a Wy musicie się do tych zmian dostosowywać. Co więcej, będąc organizacjami dynamicznie rozwijającymi się, musicie również aktualizować swoje zabezpieczenia w odniesieniu do wewnętrznych zmian oraz sposobu działania, które wdrażacie w ramach realizacji celów biznesowych. Najlepszym i jednocześnie najtańszym w długim okresie podejściem jest utrzymanie bezpieczeństwa poprzez ciągłą analizę. Ważne jest regularne badanie, które elementy zabezpieczeń wymagają modyfikacji, jakie nowe zabezpieczenia należy wdrożyć, a także z których można zrezygnować, ponieważ przestały być potrzebne lub efektywne. Warto również podkreślić, że skoro już inwestujecie czas i pieniądze w zapewnienie bezpieczeństwa swojej organizacji, dobrze jest wykorzystać te działania jako element budowania wiarygodności wobec partnerów biznesowych. Na poziomie dużych organizacji może to nie mieć aż tak dużego znaczenia, ale dla mniejszych firm to coraz ważniejszy aspekt. Wiarygodność wynikająca z wysokiego poziomu bezpieczeństwa może być decydująca, zwłaszcza gdy partnerzy biznesowi mają do wyboru dostawców oferujących podobne usługi. To może stać się jednym z kluczowych czynników wyróżniających Waszą firmę na tle konkurencji.

[01:59:15.16] - Osoba mówiąca 3

Decyzja o wyborze partnera, który zapewnia wyższy poziom bezpieczeństwa, jest dość oczywista i może stanowić istotną przewagę konkurencyjną Państwa organizacji. Najłatwiejszym sposobem uzyskania obiektywnego potwierdzenia poziomu bezpieczeństwa są programy certyfikacji. Tego rodzaju certyfikaty weryfikują standardowe elementy związane z bezpieczeństwem, skupiając się na konkretnych programach i elementach systemu zarządzania bezpieczeństwem informacji. Dzięki temu stanowią zewnętrzny i obiektywny dowód na to, że organizacja spełnia wymagania w zakresie bezpieczeństwa. Certyfikaty mogą być szczególnie przydatne w relacjach z klientami biznesowymi. Nie będzie konieczne każdorazowe przeprowadzanie audytów na ich życzenie – posiadany certyfikat sam w sobie będzie wystarczającym dowodem, że firma jest odpowiednio zabezpieczona. Na świecie istnieje wiele programów certyfikacyjnych, które mogą być wykorzystywane także przez małe i średnie organizacje. W Polsce szczególnie popularne są standardy ISO, zwłaszcza ISO 27001, który dotyczy systemu zarządzania bezpieczeństwem informacji. Certyfikacja zgodna z ISO 27001 zapewnia, że organizacja jest w stanie utrzymać ciągłość działania, nawet w obliczu potencjalnych zagrożeń. Jednakże warto podkreślić, że mimo dostosowania standardów ISO do organizacji różnej wielkości, wdrożenie ich w małych firmach może być wyzwaniem. Wynika to z konieczności spełnienia konkretnych wymagań i wdrożenia złożonych procesów, które mogą być trudne do realizacji w mniejszych strukturach. Niemniej

jednak osiągnięcie takiej certyfikacji stanowi znaczący krok w kierunku budowania zaufania i wiarygodności na rynku.

[02:01:09.02] - Osoba mówiąca 3

Podejście do certyfikacji ISO w małej firmie nie jest i nie jest łatwe. Po prostu jest podejściem dosyć dosyć kosztownym w relacji do wielkości organizacji. My zaproponowaliśmy taki program, który nazywa się firma bezpieczna cyfrowo, czyli program, który jest dedykowany do małych i średnich firm, jeśli chodzi o zdobycie takiego pierwszego certyfikatu potwierdzającego bezpieczeństwo cyfrowe. On się odnosi z założenia do podstawowych, ale najważniejszych elementów bezpieczeństwa, które wpływają na to, że Państwa organizacja będzie w stanie skutecznie bronić się przed cyber zagrożeniami. Program jest skonstruowany w taki sposób, żeby w jak najmniejszym zaangażowaniu państwa i koszcie można było uzyskać jak najwyższe efekty. W jaki sposób działa ten program? Bo nie jest to tylko czysta certyfikacja, czyli audyt i wystawienie certyfikatu. Podchodzimy w tym zakresie w sposób taki bardziej edukacyjny, czyli w pierwszym kroku zachęcamy Państwa do wypełnienia ankiety samooceny poziomu cyberbezpieczeństwa. To jest ankieta, którą się wypełnia absolutnie bezpłatnie i wynik jej macie Państwo uzyskiwany bezpośrednio. Po jej wypełnieniu. Ta ankieta dotyczy 14 sekcji, w których pytamy Państwa o tym, w jaki sposób podchodzicie do Państwa w organizacji, do różnych aspektów związanych z bezpieczeństwem.

[02:02:50.24] - Osoba mówiąca 3

W raporcie, który Państwo dostaniecie na koniec, dostajecie informację, w których obszarach jest Państwo. Działacie zgodnie ze standardami, w których wymagane są pewne zmiany i doskonalenia. Staramy się w tym raporcie. Takie odniesienie jest. Wskazujemy materiały informacyjne związane z danym zagadnieniem, w jaki sposób należy wdrożyć zagadnienia, które są u Państwa problemem. Wskazujemy też od razu rekomendacje i czynności do wykonania. Dlatego zachęcam Państwa już teraz do wypełnienia ankiety, pobrania raportu, który będzie zawierał właśnie rekomendacje co do kolejnych działań, aby uzyskać odpowiednio wysoki poziom bezpieczeństwa. Oczywiście, jeśli ta ankieta wyjdzie Państwu doskonale, to możecie Państwo od razu podchodzić do certyfikacji. Jeśli jednak będą tam jakieś braki, to należy na podstawie tego raportu przygotować odpowiedni plan doskonalenia. Jeśli Państwo czujecie się na siłach analizując ten wynik, Ten raport, że jesteście w stanie to zrobić sami. Zróbcie to sami. Jeśli potrzebujecie wsparcia, no to musicie się podeprzeć jakąś firmą ekspercką z zewnątrz, żeby rzeczywiście zabezpieczenia wdrożyć w sposób właściwy, skuteczny. Cały czas oczywiście do Państwa dyspozycji jest poradnik Firma bezpieczna cyfrowo, gdzie te wszystkie kwestie obszarów bezpieczeństwa, które są zawarte w ramach certyfikacji, są opisane w sposób szczegółowy i na podstawie których można ten plan doskonalenia stworzyć i przeprowadzić.

[02:04:30.07] - Osoba mówiąca 3

Ostatecznie, kiedy będą Państwo gotowi, możecie podpisać z nami umowę i przystąpić do procesu certyfikacji. Certyfikacja polega na weryfikacji kluczowych obszarów, które są jej przedmiotem. W tym przypadku mówimy o siedmiu obszarach cyberbezpieczeństwa dostosowanych do polskich warunków. Po pozytywnym przejściu procesu certyfikacji otrzymacie Państwo certyfikat, który potwierdzi Wasze zdolności do zapewnienia bezpiecznej współpracy z innymi podmiotami oraz ochrony Waszej organizacji. Obecnie program certyfikacji znajduje się w fazie pilotażowej, jednak wkrótce planujemy wprowadzenie akredytacji. Dzięki temu certyfikat będzie jeszcze bardziej wiarygodny i potwierdzi jakość procesu oraz konkretne zdolności Państwa organizacji w zakresie bezpieczeństwa. Teraz chciałbym przejść do kolejnej części prezentacji, dotyczącej bezpłatnych narzędzi, które mogą pomóc w podnoszeniu poziomu bezpieczeństwa lub w jego weryfikacji. Zaletą tych narzędzi jest to, że zostały one opracowane przez CERT Polska, czyli przez zespół o wysokich kompetencjach w zakresie cyberbezpieczeństwa. Są one dostępne dla Państwa i chciałbym omówić kilka z nich. Pierwsze narzędzie to **Artemis**, które bada strony internetowe udostępnione w sieci. Artemis jest standardowo wykorzystywany w podmiotach publicznych, jednak może z niego skorzystać każda organizacja, w tym również Państwa firma. Jest to praktyczne narzędzie, które może pomóc w identyfikacji potencjalnych zagrożeń związanych z bezpieczeństwem stron internetowych.

[02:06:23.20] - Osoba mówiąca 3

Wystarczy się zarejestrować pod wskazanym linkiem. Po takiej rejestracji będzie dokonany taki zdalny audyt Państwa strony internetowej. Otrzymacie Państwo raport, w którym będą wskazane elementy, które potencjalnie mogą być niebezpieczne albo niewystarczająco zabezpieczone. Na Państwa stronie. Bardzo fajne narzędzie, żeby się zorientować, jak wygląda Państwa bezpieczeństwo. Bez jeszcze bez realizacji jakichś badań specjalistycznych. Kolejne, kolejne bardzo fajne narzędzie to jest narzędzie Bezpieczna poczta. Cert.pl: To jest narzędzie, które bada, w jaki sposób skonfigurowany jest Państwa poczta. Bada m.in. czy są zaimplementowane mechanizmy, które utrudniają podszywanie się pod Państwa adresy e-mail. To jest element ważny z dwóch powodów. Po pierwsze, oczywiście, jeśli nie macie Państwo tych mechanizmów zaimplementowanych, to znajduje się tam instrukcja, jak je włączyć, jaka jest konsekwencja, jak nie korzystacie Państwo z tych mechanizmów? Konsekwencja jest taka, że część dostawców programów pocztowych przy Detekcji, że brak jest włączonych mechanizmów bezpieczeństwa dla adresacji pocztowej. Przerzuca automatycznie Wasze maile do folderu spam. Oczywiście nikomu z nas nie zależy, żeby nasza korespondencja, szczególnie biznesowa lądowała w folderze Spam naszych klientów, dlatego zachęcam do skorzystania z tego mechanizmu.

[02:08:10.06] - Osoba mówiąca 3

Kolejny element, o którym już wspominaliśmy to są smsy z linkami o charakterze phishingowym. Oczywiście nie wiemy jaki charakter jest tego linka. Oczywiście należy z bardzo dużym, z dużą rezerwą podchodzić do linków przekazywanych w SMS ach, ale każdy taki link można zweryfikować przekazując, przesyłając tę informację, nie klikając w link. Oczywiście na bezpłatne numer 880 otrzymacie Państwo informacje, czy ten link jest bezpieczny czy też nie. Kolejne narzędzie podnoszące bezpieczeństwo to lista ostrzeżeń uznanych przez CERT Polska za niebezpieczne. Jest to lista, z której korzystają najwięksi dostawcy internetu w Polsce, więc jeśli Państwo macie od nich usługę, to prawdopodobnie takie ostrzeżenia po prostu będziecie dostawać. W momencie, kiedy wejdziecie na stronę podejrzaną stronę z listy. Jeśli korzystacie z innych dostawców, to taką listę można sobie pobrać do przeglądarki i w razie czego, jeśli jakiś link przekierowowałby Państwa do takiej strony, to zostaniecie uprzedzeni, że ten link jest znajduje się na liście ostrzeżeń CERT Polska. Jeśli chodzi o strony uznane za niebezpieczne. Kolejne narzędzie to już dla firm bardziej zaawansowanych, które posługują się własną pulą adresów IP.

[02:09:39.14] - Osoba mówiąca 3

To usługa, dzięki której przedsiębiorstwa mogą uzyskać informacje o problemach związanych z bezpieczeństwem, infrastrukturą oraz potencjalnymi zagrożeniami dotyczącymi ich adresacji IP. Narzędzie to, dostępne bezpłatnie, korzysta z wielu silników zbierających informacje o bezpieczeństwie w sieci, co czyni je wartościową opcją dla organizacji chcących monitorować swoje środowisko IT. Ostatnim narzędziem, które chciałbym omówić, jest dedykowane dla tych, którzy otrzymują oprogramowanie i nie są pewni, czy jest ono bezpieczne. Umożliwia ono przesyłanie takich plików do repozytorium przeznaczonego do przechowywania próbek złośliwego oprogramowania. Dzięki temu można bezpiecznie otworzyć próbkę w kontrolowanym środowisku i przeanalizować jej działanie. Warto jednak pamiętać, że w celu skorzystania z tej usługi wymagana jest rejestracja. Zachęcam również do zgłaszania incydentów i zdarzeń, które mogą Państwa niepokoić, za pośrednictwem kanałów udostępnionych przez CERT Polska. Jako małe i średnie przedsiębiorstwa w 99% przypadków podlegacie pod ten zespół, co czyni go właściwym miejscem do zgłaszania potencjalnych problemów. Jest to szczególnie istotne w sytuacjach, gdy w organizacji brakuje wykwalifikowanego personelu, który mógłby ocenić, czy dane zdarzenie jest incydentem, czy jedynie wynikiem innych czynników, takich jak problemy z wydajnością sprzętu. W przypadku mniej oczywistych objawów, takich jak np. nagłe spowolnienie działania urządzeń, trudno samodzielnie określić, czy to efekt ataku, czy zwykłe kwestie techniczne. CERT Polska jest w takich sytuacjach doskonałym wsparciem.

[02:11:44.01] - Osoba mówiąca 3

Także polecam tego, żeby incydenty zgłaszać. Duże organizacje są zobowiązane do tego, żeby zgłaszać incydenty. W związku z tym w tych statystykach, które państwu pokazaliśmy. Te incydenty z dużych organizacji zawsze są. Te incydenty od państwa są rzadziej, dlatego że nie zawsze państwo zgłaszacie je do CerTu I przy okazji, ponieważ słowo ransomware przewija się przez nasze prezentacje, przewijało się już kilkukrotnie. Chciałem Państwa zachęcić do tego, żebyście Państwo. Przejrzeli dokument przygotowany specjalnie dla małych i średnich przedsiębiorstw dotyczących. Poradnik dotyczący ransomware od początku do końca. Jak się zabezpieczać przed ransomware? Co robić w momencie, kiedy taki atak ma miejsce na Państwa organizacje? No to jest na pewno coś, co Państwu może pomóc uniknąć takiego ataku i zadziałać odpowiednio w momencie, kiedy atak będzie miał miejsce. Podsumowując. Nie robi się bezpiecznej. Ilość wyrafinowanych cyber zagrożeń się zwiększa. Te zagrożenia zmieniają swój charakter, są coraz bardziej trudne do odróżnienia od poprawnej aktywności, działań, działań w sieci. W związku z tym trzeba zachować dużą czujność. Trzeba zachować cyber higienę, czyli? Czyli mieć świadomość tego, co może być atakiem, co co nie.

[02:13:22.24] - Osoba mówiąca 3

Bardzo ważne jest, aby mieć świadomość obszarów wymagających ochrony, ponieważ to właśnie one pozwalają Państwu podejmować rozsądne i przemyślane decyzje biznesowe, w tym decyzje dotyczące wdrażania zabezpieczeń. Te zabezpieczenia powinny być zarówno racjonalne, jak i skuteczne. Cyberbezpieczeństwo może stać się elementem przewagi konkurencyjnej, szczególnie w sektorze małych i średnich przedsiębiorstw, i warto tę przewagę wykorzystać. Jest to aspekt, który będzie odgrywał coraz większą rolę w budowaniu trwałych relacji biznesowych.Certyfikacja stanowi uniwersalne i relatywnie niedrogie rozwiązanie, które może potwierdzić spełnienie wymagań w zakresie cyberbezpieczeństwa. Warto korzystać z wiarygodnych mechanizmów wspierających ochronę firmy oraz wdrażać narzędzia, które dzisiaj Państwu zaprezentowałem.
Z mojej strony to wszystko. Bardzo dziękuję za uwagę.

[02:14:21.11] - Osoba mówiąca 1

Panie Piotrze, Również bardzo dziękuję. I podobnie jak Pani Anna, w sposób wyczerpujący przedstawił Pan nam to zagadnienie, to znaczy firmy bezpiecznej cyfrowo. Niemniej jednak zawsze chodzi o szczegóły. Proszę pozwolić mi dopytać o jedną rzecz. Zauważyłem w Pana prezentacji dane dotyczące tego, że wśród osób, które narażają firmę na cyberatak, są byli niezadowoleni pracownicy, co stanowi całkiem sporą grupę. Jak firma, jak przedsiębiorca może podejść do tego zagadnienia? To znaczy, co należy zrobić? Jaki jest pierwszy krok? Jeżeli z firmy odchodzi pracownik, który miał dostęp do danych wrażliwych, ewentualnie cały zespół pracujący na takich danych, co powinno się zrobić tego samego dnia i w ciągu kolejnych dni?

[02:15:11.07] - Osoba mówiąca 3

To jest proces złożony. On nie powinien się zaczynać w tym momencie. Dlatego, że pierwszą, najważniejszą rzeczą jest oczywiście zastosowanie mechanizmów bezpieczeństwa przy dostępie do danych. Nadawanie właściwych uprawnień to jest element, który powoduje, że wiemy, kto nad jakimi danymi pracuje, kto i gdzie ma dostęp. To jest element podstawowy. Drugi dostęp to zapewnienie oczywiście odpowiedniego postępowania z danymi, czyli odpowiednie procedury i weryfikacja ich przestrzegania. Kolejny element oczywiście to jest taki, że w momencie, kiedy pracownik żegna się z firmą, to oczywiście, żeby w odpowiednim momencie odpowiedni dostęp do danych zostały też oczywiście odebrane, żeby nie było takiej sytuacji. Oczywiście rozstania bywają bardzo różne i trzeba się liczyć z tym, że że mogą się z tym wiązać jakieś jakieś nieprzyjemności. Jeśli firma generalnie systemowo podchodzi do zagadnień bezpieczeństwa, to takich problemów po prostu być nie powinno.

[02:16:14.08] - Osoba mówiąca 1

Zmieniłby Pan hasło? Jeszcze dopytam. Hasła dostępu do komputerów w biurze na przykład.

[02:16:21.11] - Osoba mówiąca 3

Tutaj się po prostu odbiera dostęp. To nie jest kwestia zmiany hasła, Tak.

[02:16:26.21] - Osoba mówiąca 1

Bardzo dziękuję za odpowiedź na to pytanie.

[02:16:28.19] - Osoba mówiąca 3

Każdy powinien mieć indywidualne hasło. To jest inna sprawa.

[02:16:32.07] - Osoba mówiąca 1

Ale przejdźmy teraz do pytań, które zadają nam nasi odbiorcy, Bo rzeczywiście docierają do nas takie pytania. I tutaj na początku jako pierwsze oddamy głos pani Grażynie. Zapytała nas, jak powinien zachować się pracownik, który przypadkowo kliknął w link. No najprostsza rzecz prawda, która może się zdarzyć. Nie należy go czy jej w jakiś sposób piętnować, prawda? Tak.

[02:16:56.02] - Osoba mówiąca 2

Myślę, że bardzo ważne jest to, co mówiłam w trakcie prezentacji, że warto w firmie promować taką kulturę bezpieczeństwa, żeby pracownicy wiedzieli, że jeśli coś się zadziało, czyli jeśli kliknęłam w link, to mam prawo to zgłosić, A może nawet nie tyle prawo, co obowiązek zgłosić, że doszło do takiego działania. Jeśli wprowadzimy, będziemy prowadzić taką politykę, że pracownicy się będą bali przyznać do błędu, czy to będzie kliknięcie w link czy cokolwiek innego, no to niestety tak naprawdę zamiast zareagować w odpowiednim momencie i podjąć działania, które być może by zatrzymały jakiś zaawansowany atak na naszą organizację. Tak naprawdę może dojść do tej sytuacji, że przeoczymy ten moment, kiedy powinniśmy podjąć właściwe działania. Także zachęcam do tego, że jeśli Państwo kliknęliście w link, przypadkowo pobraliście fakturę, czy myśleliście, że wygraliście iPhone'a, zgłoście to jak najszybciej do swoich przełożonych. Zgłoście to jak najszybciej do działu bezpieczeństwa, jeśli posiadacie taki w organizacji, bo dzięki temu jesteśmy w stanie odpowiednio zareagować w odpowiednim momencie, zatrzymać atak i podjąć działania, które mogą zmniejszyć jego skutki.

[02:18:00.19] - Osoba mówiąca 1

A jeżeli to jest jednoosobowa działalność gospodarcza?

[02:18:04.05] - Osoba mówiąca 2

Przede wszystkim zachęcam mimo to do klikania w linki. Jeśli zdarzyło nam się kliknąć i mamy podejrzenia, że coś się dzieje z naszym komputerem, zachęcam do tego, aby przeskanować go sobie przede wszystkim programem antywirusowym. Jeśli mamy podejrzenia, że coś się dzieje, a nie mamy fachowej wiedzy takiej komputerowej, zachęcamy skontaktowanie się już z jakąś firmą obsługującą tego typu rozwiązania, żeby rzeczywiście sprawdziła, czy z naszym sprzętem jest wszystko w porządku.

[02:18:31.08] - Osoba mówiąca 1

Przyznam, że kiedyś natrafiłem na badania pokazujące, że ludzie wciąż, pomimo ostrzeżeń i próśb ze strony ekspertów, używają bardzo prostych haseł, takich jak „1234567” czy „małpa wykrzyknik”. To rodzi pytanie, które zadała pani Aneta: co należy rozumieć pod pojęciem słabego hasła, a co pod pojęciem mocnego hasła? Kto z Was chciałby na to odpowiedzieć?

[02:18:59.18] - Osoba mówiąca 2

No tutaj, gdy mówimy o hasłach, to – tak jak mówiłam w trakcie prezentacji – pamiętajmy, że im hasło dłuższe, tym lepsze. Starajmy się unikać wzorów na klawiaturze, jakichś tam trójkątów, kwadratów czy innych schematów, bo są to hasła, które często pojawiają się w wyciekach. Unikajmy haseł związanych z naszą osobą, czyli nie twórzmy ich na podstawie swojego imienia, nazwiska, daty urodzenia czy imienia ulubionego zwierzaka, ponieważ tego typu informacje

często publikujemy w sieci, a cyberprzestępcy mogą je łatwo wykorzystać. Nie twórzmy też haseł składających się z przypadkowego wyrazu i dodanych do niego cyfr, ponieważ takie hasła również są łatwe do złamania. Starajmy się używać kombinacji kilku wyrazów, np. można stworzyć jakąś frazę, na przykład: „Dwa czerwone naleśniki jadą na zielonym rowerze”. Proszę już nie

[02:19:54.24] - Osoba mówiąca 1

Używać tego hasła?

[02:19:55.23] - Osoba mówiąca 2

Absolutnie, proszę wymieniać i mieszać różne elementy. Twórzmy takie hasła, które będą dla nas łatwe do zapamiętania, a jednocześnie kojarzyły się tylko nam. Unikajmy prostych schematów, takich jak jeden wyraz pisany od tyłu czy od przodu, ponieważ takie hasła są łatwe do złamania. Tak jak wspominałam podczas prezentacji, zachęcam do korzystania z menedżerów haseł, ponieważ pomagają one tworzyć i zabezpieczać silne hasła. Dodatkowo przypominam o włączeniu weryfikacji dwuetapowej w każdej usłudze. Nawet jeśli nasze hasło wycieknie, cyberprzestępcy nie będą w stanie uzyskać dostępu bez podania dodatkowego kodu.

[02:20:29.08] - Osoba mówiąca 1

Zauważyłem, że jeśli chodzi o menedżera haseł, to jest wiedza, którą Pani systematycznie utrwala podczas tego webinaru, i to z pewnością wyjdzie nam wszystkim na dobre. Pan Marek pyta o Windows Defendera, a dokładniej – czy ten system, który jest dostępny od razu po instalacji systemu operacyjnego, jest wystarczający, aby zapewnić stuprocentową cyberochronę?

[02:20:55.06] - Osoba mówiąca 3

No to każdy specjalista bezpieczeństwa powie państwu, że nie ma stuprocentowej ochrony. Natomiast Natomiast my nie oceniamy poszczególnych systemów. Są organizacje, które, które porównują różne rozwiązania bezpieczeństwa i są z tymi ekspertami. Warto sobie spojrzeć i porównać funkcjonalności. Skuteczność. Te wszystkie dane są dostępne w takich raportach z porównań i odpowiedzieć na pytanie, czy z naszego punktu widzenia to zawsze. Zawsze mówię o tym, że nasz apetyt na ryzyko jest tym, który decyduje. Być może Windows Defender będzie właśnie to, co będziemy chcieli, a być może będziemy chcieli inne rozwiązanie. Tutaj ważne jest, żeby żeby nie wyłączyć Windows Defendera, jeśli się nie ma innego zabezpieczenia na komputerze. Tak może być.

[02:21:44.04] - Osoba mówiąca 1

I chyba chodzi też o aktualizacje systemowe. Aktualizacje równocześnie aktualizują właśnie Defendera i w związku z tym trzeba też to robić.

[02:21:53.02] - Osoba mówiąca 3

Każde rozwiązanie znaczy najważniejszy element jest taki, żeby. Oczywiście oprogramowanie, z którego korzystamy, niezależnie czy to jest oprogramowanie systemowe, czy to jest to są programy funkcjonalne, czy oprogramowanie służące ochrony naszego komputera, żeby one zawsze były wspierane, czyli żebyśmy mieli czy producent dalej wspierał to rozwiązanie, żebyśmy mieli Aktualnie aktualne aktualizacje, bo to jest podstawa do tego, żeby te systemy po prostu spełniały swoją funkcję.

[02:22:24.14] - Osoba mówiąca 1

A teraz pytanie od Pani Natalii. Pani Natalia pyta, jak prawidłowo i należycie zabezpieczyć swój komputer. Czy myślimy tutaj równocześnie o hardware i software? Tak, tak, to właśnie jest intencją pytania. Moglibyśmy prześledzić drogę – załóżmy laptopa – od domu do biura, a ewentualnie jeszcze podczas zakupów. Jak należy podchodzić do ochrony sprzętu?

[02:22:54.24] - Osoba mówiąca 3

No, jeśli chodzi o zabezpieczenia fizyczne, to chyba nie będziemy o tym mówili. To oczywiście po prostu trzeba pilnować swojego laptopa. Tak? I nie zostawiać w bagażniku samochodu idąc na zakupy.

[02:23:06.22] - Osoba mówiąca 3

Zabezpieczać należy zgodnie z zasadami ustalonymi przez firmę, jeśli jest to urządzenie służbowe. Natomiast w przypadku urządzeń prywatnych należy to zrobić w sposób, który uznajemy za odpowiedni. Kluczowe jest jednak nie tylko zabezpieczenie fizyczne – choć oczywiście dbamy o to, by urządzenie było odpowiednio przechowywane – ale przede wszystkim regularne aktualizowanie oprogramowania i korzystanie ze wspieranego sprzętu. Ważne jest, aby zawsze mieć włączonego antywirusa oraz upewnić się, że wszystkie programy i system operacyjny są aktualne. To podstawowe elementy, które zapewniają prawidłowe działanie urządzenia i podnoszą jego bezpieczeństwo. Warto pamiętać, że nie wszystkie aktualizacje są automatyczne. Jeśli korzystamy z oprogramowania, które wymaga ręcznego aktualizowania, powinniśmy regularnie weryfikować, czy nie pojawiły się nowe poprawki i instalować je na bieżąco.

[02:24:05.03] - Osoba mówiąca 1

Niektóre komercyjne programy antywirusowe dają kolejne stopnie zaawansowania, update'y. Związane jest to oczywiście też z ceną. Jak podejść do tego? To znaczy czy zawsze starasz się być na górze, że tak powiem, oczekiwań i i też zaawansowania? Czy można sobie pozwalać na środkowe wersje, opcje?

[02:24:26.17] - Osoba mówiąca 3

Znaczy na pewno trzeba mieć jakieś zabezpieczenie, a to jakie? Zazwyczaj kolejne wersje oprogramowania są wyposażone w dodatkowe funkcje. I to jest pytanie o to, czy dodatkowe funkcje będziemy wykorzystywać, czy nie będziemy wykorzystywać. Tutaj jakby to jest takie racjonalne podejście, podstawowe zadanie każdego, każdego z tych z tych mechanizmów, Czyli jeśli mówimy o zabezpieczeniu, które chociażby chroni nas przed wirusami, to ono będzie takie same na każdym poziomie, natomiast będziemy mieli dodatkowe elementy, które wzbogacą nasze bezpieczeństwo, np. Dodatkowe możliwość zestawienia sesji VPN albo tego typu rozwiązań. Ważne jest, żeby jakieś aktualne zabezpieczenie było.

[02:25:13.05] - Osoba mówiąca 1

Cały czas to powtarzamy. I rzeczywiście to jest fundament architektury, bezpieczeństwa i prywatnego, i też w firmie. A ja zachęcam państwa cały czas do tego, żeby aktywnie przyłączyć się do naszej rozmowy i nawet w tym momencie wykorzystać klawiaturę swojego w pełni zabezpieczonego komputera i wysłać nam pytanie bądź komentarz do tego, o czym rozmawiamy. I rzeczywiście taki komentarz do komentarza pojawił się ze strony Pana Dawida. Jaki menadżer haseł Państwo rekomendujecie? To jest z pewnością pytanie do Pani, do Pani Anny, ponieważ pani Anna prowadziła ten wątek.

[02:25:46.09] - Osoba mówiąca 2

Tutaj, podobnie jak Piotr odpowiadał w kontekście programów antywirusowych, jakie powinniśmy wybrać. My też zachęcamy do tego, aby zapoznać się z ofertą na rynku, zastanowić się, jaki menedżer haseł będzie dla mnie odpowiedni, czy na przykład biorę taki, który zapisuję hasła w chmurze, czy wybieram taki, który zapisuje hasła lokalnie? To już decyzja do państwa. My jako NASK nie podajemy konkretnych nazw konkretnych produktów, jaki wybrać należy do Państwa decyzji. Zachęcamy do tego, aby z nich korzystać. A to jaki byłby odpowiedni i najlepszy dla Państwa musicie już zdecydować sami. Na rynku też, tak jak Piotr wspomniał, są organizacje, które zajmują się robieniem różnego rodzaju rankingów. Sprawdzanie, który który menedżer haseł jest lepszy, który gorszy. Dlatego to już jest państwa decyzja. Ja zachęcam do tego, żeby

z nich korzystać. Dodam też, że te dostępne w przeglądarkach czy w naszych urządzeniach telefonicznych są bezpieczne i jeśli wystarczy Wam do takiej codziennego użytkowania to, co jest w naszej przeglądarce, w naszym urządzeniu telefonicznym może on zostać. Jeśli potrzebujecie Państwo więcej ochrony, można się zapoznać z ofertą na rynku.

[02:26:57.20] - Osoba mówiąca 1

W prezentacji Pana Piotra wychwyciłem też informację o raportowaniu incydentów, że nie zawsze jest tak, że firma rzeczywiście raportuje i w ten sposób Niejako buduje w ogóle system bezpiecznego biznesu w całym kraju. Dlaczego to jest konieczne? Dlaczego należy o to zadbać?

[02:27:17.19] - Osoba mówiąca 3

To jest konieczne z dwóch powodów. Po pierwsze, warto zaraportować taki incydent, żeby poszukać wsparcia, jeśli chodzi o sposób postępowania z nim. Po drugie, to daje też przegląd tego, co się dzieje na rynku, co się dzieje w infosferze dla organów, które są odpowiedzialne za to, żeby podejmować odpowiednie akcje. Oczywiście na poziomie już kraju czy regionu. I to są to są elementy, które są kluczowe. Musimy budować sobie świadomość o tym, jakiego typu są nowe ataki, żebyśmy mogli państwa przed nimi ostrzegać.

[02:27:53.19] - Osoba mówiąca 1

To raportowanie jest automatyczne? To nie jest tak, że trzeba do tabeli Excel wpisywać datę i formularz?

[02:28:03.21] - Osoba mówiąca 3

To jest formularz, w którym należy podać pewne dane. Oczywiście, im więcej informacji jesteście w stanie dostarczyć na wstępie, tym lepiej. Jednak w niektórych sytuacjach może być tak, że nie wszystko jest od razu wiadomo. Dołączenie podejrzanego pliku do zgłoszenia to rekomendacja, którą CERT Polska udostępnia. Na stronie CERT Polska znajduje się dokładne wyjaśnienie, jak postępować w określonych sytuacjach.

[02:28:32.13] - Osoba mówiąca 1

I to prawda, że nie można się zabezpieczyć w 100%. Jak pan wspomniał chwilę temu, ryzyko zawsze istnieje, a aby dobrze zabezpieczyć swoją działalność biznesową i firmę, należy ustalić poziom ryzyka, który jesteśmy w stanie zaakceptować. Czy dobrze zrozumiałem takie podejście? Jeśli tak, to jak wyznaczyć sobie ten poziom akceptacji ryzyka?

[02:29:01.07] - Osoba mówiąca 3

No to jest bardzo różnie, w zależności od rodzaju biznesu, to jest chociażby w planach ciągłości działania. To jest ustalenie prostej przyczyny, ile czasu jesteśmy w stanie działać bez danego systemu, ile w stanie firma jest w stanie przetrwać bez jakiś elementów, które wpływają chociażby na jej wynik finansowy. No bo wiadomo, że na pewnym etapie to jest bankructwo. I to jest bardzo specyficzne, oczywiście dla każdej organizacji i na poziomie takiego dużego parametru jak czy firma przetrwa, czy nie, jak również na poziomie parametrów znacznie niższych, czyli tych bez, bez jakiego elementu możemy się obyć przez jakiś czas z zaakceptowanym skutkiem?

[02:29:49.05] - Osoba mówiąca 1

A jeśli chodzi o przechowywanie danych i w ten sposób o zabezpieczanie się przed sytuacjami, które już nastąpią. Załóżmy, że firma stoi w obliczu zablokowania danych, To lepiej trzymać na zewnętrznych dyskach. Czy lepiej zdecydować się na chmurę? Co Pani rekomendowała by w tej sytuacji?

[02:30:08.21] - Osoba mówiąca 2

Tak naprawdę wszystko zależy od tego, jak dużo danych posiadacie. Czy potrzebujecie Państwo dużej serwerowni, czy może wystarczy chmura? Rozwiązania w chmurze są bezpieczne, choć wycieki mogą zdarzyć się zarówno w przypadku danych przechowywanych w chmurze, jak i na dyskach lokalnych. To kwestia tego, co dla Państwa jest bardziej wygodne – czy macie odpowiednią przestrzeń, jak dużo danych posiadacie i w jaki sposób chcecie mieć do nich dostęp. Jeśli przechowujecie dane w chmurze, to dostęp do nich możecie mieć z każdego miejsca. Natomiast przy korzystaniu z dysków lokalnych lub stacjonarnych możliwości dostępu są bardziej ograniczone. Decydując, gdzie i w jaki sposób przechowywać dane, warto wziąć pod uwagę te aspekty i wybrać rozwiązanie najlepiej odpowiadające Waszym potrzebom.

[02:31:03.01] - Osoba mówiąca 1

A teraz jeszcze proszę pochwalcie się, gdzie można znaleźć informacje, które przedstawiliście w Waszych prezentacjach. Głównie myślę o linkach do odpowiednich formularzy, do poradnika, do. Też informacje na temat darmowego sposobu sprawdzania systemów bezpieczeństwa w firmie.

[02:31:25.19] - Osoba mówiąca 2

Jeśli chodzi o materiały edukacyjne, które gorąco polecam, to przede wszystkim strona **BezpiecznyMiesiąc.pl**. Zachęcam również do odwiedzenia strony zespołu **CERT Polska**, gdzie znajdziecie Państwo mnóstwo informacji o narzędziach i rozwiązaniach, o których wspominał

Piotr. Na stronie CERT Polska, po kliknięciu w „zgłoś incydent," zostaniecie przekierowani na odpowiednią stronę, gdzie można wypełnić formularz i zgłosić ewentualny incydent. Zachęcam też do odwiedzenia strony **Firma Bezpieczna Cyfrowo**, również omawianej przez Piotra, ponieważ znajdziecie tam ogrom materiałów, które mogą pomóc w zadbaniu o bezpieczeństwo zarówno firmowe, jak i prywatne. Warto w tym cyfrowym świecie nieustannie podnosić swoje kompetencje. Myślę, że to wszystko, co chciałam przekazać.

[02:32:17.05] - Osoba mówiąca 1

Pani Anna Kwaśniak, pan Piotr Ławniczak, bardzo dziękuję. Zaraz po webinarze będziemy wdzięczni za Państwa opinie – otrzymacie ankietę, którą prosimy wypełnić od razu, ponieważ sprawy odkładane na później często pozostają niezałatwione. A co wydarzy się w ramach **Business Digital** w najbliższych dniach? Już w przyszłym tygodniu, 22 stycznia, odbędzie się drugie z serii webinarów pod tytułem „Rozwijaj swój biznes dzięki nowoczesnym technologiom cyfrowym." Tym razem będzie więcej o usługach, a także o skalowaniu biznesu, co – jestem przekonana – zainteresuje Państwa równie mocno jak dzisiejsze spotkanie. Liczymy na równie dużą, jeśli nie większą, frekwencję. Natomiast 24 stycznia zapraszamy na spotkanie stacjonarne w Mrągowie. Tam na pewno będzie się działo! Będzie to okazja, aby osobiście zadać mnóstwo pytań ekspertom i na żywo uzyskać odpowiedzi na temat radzenia sobie z cyberzagrożeniami. Spotkanie to będzie rozwinięciem dzisiejszego tematu i pozwoli jeszcze bardziej zgłębić omawiane kwestie. Bez wątpienia będzie to doskonała okazja do pogłębienia wiedzy i zadawania pytań, którą warto w pełni wykorzystać.

[02:33:34.24] - Osoba mówiąca 1

Więcej informacji na temat tego, co dzieje się w ramach Business Digital, znajdziecie Państwo na stronie business.gov.pl/digital. Bardzo dziękuję za dzisiejsze spotkanie i do zobaczenia wkrótce!