NOWE TECHNOLOGIE W MEDYCYNIE

Wiedza kluczem do cyberbezpieczeństwa

Nowoczesne technologie odgrywają coraz większą rolę w medycynie. Bez narzędzi cyfrowych dzisiaj nie wyobrażamy sobie funkcjonowania całego systemu ochrony zdrowia, co jeszcze kilka dekad temu było nie do pomyślenia. Wraz z postępem rosną jednak także cyfrowe zagrożenia. O tym, jak się przed nimi ustrzec, rozmawiamy z Michałem Zdunowskim, założycielem firmy IS Consulting specjalizującej się w tworzeniu spersonalizowanych strategii cyberbezpieczeństwa.

Postępująca cyfryzacja usług medycznych i wykorzystywanie w sektorze ochrony zdrowia nowoczesnych technologii z jednej strony oznaczają większą efektywność systemu, ale z drugiej większą podatność na zagrożenia cybernetyczne. W jakim miejscu pomiędzy postępem technologicznym a kreowanymi przez ten postęp niebezpieczeństwami obecnie się znajdujemy?

W ostatnich latach, szczególnie pod wpływem pandemii, postęp technologiczny w sektorze ochrony zdrowia znacząco przyspieszył, przyjmując formę skokowego wzrostu. Widoczne było globalne zwiększenie wykorzystania usług chmurowych, co doprowadziło do migracji danych pacjentów i innych systemów z lokalnych centrów danych do infrastruktury chmurowej. To z kolei wpłynęło na cyberbezpieczeństwo – firmy posiadające wyrafinowane technologicznie rozwiązania, takie jak Microsoft, Amazon czy Google, znacząco podniosły ochronę systemów i przetwarzanych danych. Mimo to statystyki pokazują ciągle rosnącą liczbę cyberataków na sektor ochrony zdrowia. Według szacunków Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) 8 proc. wszystkich incydentów dotyczyło sektora ochrony zdrowia, który był trzecim najczęściej atakowanym sektorem. Aż 80 proc. ataków rozpoczęło się od działań socjotechnicznych, co podkreśla znaczenie edukacji pracowników w zakresie identyfikacji i zgłaszania potencjalnych zagrożeń. To jest kluczowe dla ochrony organizacji, pacjentów oraz pracowników.

Jak twierdził słynny haker Kevin Mitnick, „to ludzie, a nie technologie, są najsłabszym ogniwem bezpieczeństwa". Jak przygotowani są pracownicy ochrony zdrowia, którzy na co dzień korzystają ze zdobyczy technologicznych, do tego, aby być pierwszą linią obrony przed zagrożeniami cybernetycznymi?

Trudno się z tym nie zgodzić, aczkolwiek należy pamiętać, że za technologią też stoją ludzie. Osobiście pokusiłbym się o stwierdzenie, że to styl życia, jaki prowadzimy w ostatnim czasie, w największym stopniu przyczynił się do pogorszenia ogólnego stanu cyberbezpieczeństwa. Rosnący trend pracy zdalnej oraz wszechobecny stres i pośpiech to czynniki bezpośrednio wpływające na zwiększoną liczbę ataków.

Pracownicy ochrony zdrowia stają się pierwszą linią obrony przed hakerami wykorzystującymi elementy psychologii strachu, pilności czy zmęczenia. Przykład ataku na firmę diagnostyczną ALAB z 19 listopada 2023 r., który skutkował wyciekiem ponad 270 tys. rekordów, pokazuje, jak socjotechnika może być użyta do wpuszczenia *ransomware*, a następnie zaszyfrowania i kradzieży danych. Hakerzy często inicjują swoje ataki przez fałszywe e-maile, wysyłając *malware* w załącznikach w postaci faktury lub linku do spreparowanej strony.

Dlatego tak istotne jest, by pracownicy ochrony zdrowia byli świadomi oraz przestrzegali podstawowych zasad cyberhigieny: używania antywirusów, dokonywania regularnych aktualizacji, weryfikacji podejrzanych maili i stosowania nowoczesnych metod uwierzytelniania. Podobnie jak rutynowe mycie rąk przed zabiegiem – te proste działania mogą radykalnie zwiększyć ich bezpieczeństwo oraz bezpieczeństwo pacjentów w cyberprzestrzeni. To podkreśla ich rolę jako pierwszej linii obrony.

> *Pracownicy ochrony zdrowia stają się pierwszą linią obrony przed hakerami wykorzystującymi elementy psychologii strachu, pilności czy zmęczenia. Dlatego tak istotne jest, by przestrzegali podstawowych zasad cyberhigieny*

Bez wątpienia rośnie świadomość, że aby tworzyć bezpieczeństwo w sektorze ochrony zdrowia, obok odpowiednich narzędzi konieczna jest przede wszystkim wiedza. Nie tylko informatyków, ale pracowników każdego szczebla. W jaki sposób budować wśród nich świadomość zagrożeń i zasad, których trzeba bezwzględnie przestrzegać?

Jak wynika z danych od naszych partnerów technologicznych, podatność na ataki socjotechniczne w sektorze wynosi średnio 38,2 proc. w organizacjach, które nie wdrożyły żadnego planu szkoleniowego. Efekty wprowadzenia takiego programu widać już po 90 dniach – średnio ten odsetek spada do 19,5 proc. Długofalowe programy mogą zmniejszyć ryzyko ataku aż do 5,1 proc.

Już jakiś czas temu zauważyliśmy, że suche programy szkoleniowe, które nie angażują aktywnie w proces budowania świadomości, nie zdają egzaminu. Żeby program był skuteczny, musi wpływać bezpośrednio na emocje osoby szkolonej. Aby taki cel osiągnąć, można wykorzystać specjalne

Fot. Archiwum

> *Im wcześniej jako organizacja wykryjemy incydent, tym większe szanse na to, że uda nam się rozwiązać problem przed powstaniem większej szkody*

platformy e-learningowe, dzięki którym możemy nie tylko przypisywać tematyczne szkolenia, lecz także angażować pracowników do współzawodnictwa w grach, oglądania miniseriali, a nawet do symulacji ataków.

Tego typu platformy pozwalają też na pełną personalizację szkoleń, dzięki czemu możemy opracować konkretne szkolenia dla konkretnych działów po wcześniej analizie ich pracy. Możemy zweryfikować, na jakie ataki pracownicy są najbardziej narażeni, tak aby szkolenie było maksymalnie efektywne. Prowadząc szkolenia w firmach, zawsze staramy się proponować interaktywne warsztaty, dzięki czemu uczestnicy mają okazję zobaczyć od kuchni, jak łatwo jest przeprowadzić atak oraz ile wysiłku wymaga zniwelowanie skutków takiego incydentu.

Niestety, cyberataki zdarzały się, zdarzają i będą się zdarzać. Przestępcy są niejednokrotnie wyposażeni w najnowsze technologie i urządzenia, mają specjalistyczną wiedzę. Jak reagować na takie incydenty, jak minimalizować ich skutki?

To prawda. Hakerzy wykorzystują nowoczesne technologie, często zanim my będziemy mogli je wykorzystać – świetnym przykładem jest AI. Dlatego tak ważne jest proaktywne działanie, które nie polega tylko na wdrażaniu nowoczesnych technologii, ale również na przygotowaniu organizacji na incydent. Podstawowym problemem jest pierwszy krok, czyli identyfikacja incydentu.

O ile na co dzień technologia wspomaga nas przy identyfikacji incydentów w systemach, o tyle w przypadku ataków socjotechnicznych to właśnie użytkownik jest kluczowym elementem całej układanki. Pracownicy bardzo często nie raportują incydentów i jest ku temu kilka przesłanek: strach przed konsekwencjami, wstyd z powodu popełnienia błędu, zbyt skomplikowane procedury raportowania. To najczęstsze przypadki, z jakimi się spotykamy.

Podstawową reakcją na każdy incydent jest zgłoszenie do odpowiedniego działu, niezależnie od tego, jak wstydliwy czy błahy jest powód. W sprawę incydentu zaangażowana jest cała organizacja, dlatego kultura i otwartość organizacji mają taki sam priorytet jak prostota procedur zgłaszania incydentów. Im wcześniej jako organizacja wykryjemy incydent, tym większe szanse na to, że uda nam się rozwiązać problem przed powstaniem większej szkody.

Wiedza o cyberzagrożeniach i o tym, jak się przed nimi ustrzec, to nie tylko bezpieczeństwo pracowników, pacjentów i baz danych, gromadzonych powszechnie w systemie. To także inne korzyści. Jakie?

Nowoczesne technologie na dobre rozgościły się w naszych domach. Inteligentne urządzenia, takie jak telewizor, smartwatch czy nawet lodówka, zbierają dane o naszych upodobaniach, przyzwyczajeniach, a także o stanie zdrowia. Informacje o tym, gdzie mieszkamy, gdzie pracujemy, jakie stanowiska piastujemy, są publicznie dostępne w serwisach Facebook czy Linkedin.

Do tej mieszanki wystarczy dodać fakt, że w większości serwisów korzystamy do logowania z naszego maila – i tragedia czyha za rogiem, na własne życzenie. Zdobyte umiejętności, wiedzę i nawyki bardzo łatwo możemy wdrożyć w życie domowe, dzięki czemu zmniejszamy swój ślad cyfrowy, zwiększając prywatność naszą i naszych najbliższych. Umiejętność tworzenia silnych haseł pozwala na zabezpieczenie domowych urządzeń przed przechwyceniem i wywołaniem awarii.

Jeśli już padniemy ofiarą ataku, wiedza o tym, gdzie należy się zgłosić, zwiększy nasze szanse na odzyskanie utraconych pieniędzy lub danych. Z cyberświatem jest trochę jak z przechodzeniem przez ulicę – jeśli nauczymy się, że przed wejściem na pasy należy zawsze spojrzeć w lewo, później w prawo i znów w lewo, to zwiększamy szanse, że nie wpadniemy pod samochód, nawet jeśli mamy zielone światło. Co ważniejsze, nie trzeba być zawodowym kierowcą, żeby znać podstawowe zasady ruchu drogowego.

Asklepios to postać z mitologii greckiej, bóg medycyny i uzdrowienia. To także metafora ochrony danych i systemów przed zagrożeniami cyfrowymi, która jest realizowana w projekcie ASCLEPIUS współfinansowanym ze środków unijnych. Jakie są założenia tego projektu, jak wygląda jego realizacja, jakie przynosi korzyści?

W listopadzie 2023 r. uruchomiliśmy autorski projekt ASCLEPIUS, którego celem jest wdrożenie nowoczesnych technologii cyberbezpieczeństwa właśnie w sektorze ochrony zdrowia. Jednym z kluczowych celów jest poprawa wiedzy i świadomości w zakresie cyberbezpieczeństwa wśród pracowników ochrony zdrowia.

Dzięki środkom z programu Cyfrowa Europa pracownicy będą mogli się zapisać na szkolenia i warsztaty w ramach naszej Akademii CyberSkills, aby zwiększyć swoje kompetencje w zakresie cyberbezpieczeństwa. Dodatkowo dla pracowników IT ochrony zdrowia przygotowaliśmy specjalne szkolenia przygotowujące do zdobycia renomowanych certyfikatów wraz z voucherami na egzaminy. Mamy również specjalną ofertę dla organizacji ochrony zdrowia, którym dajemy dostęp do nowoczesnej platformy e-learningowej rynkowego lidera.

> *Dzięki udziałowi w projekcie ASCLEPIUS aktywnie wspomagamy sektor ochrony zdrowia w zdobywaniu wiedzy i kompetencji potrzebnych do funkcjonowania w nowoczesnym cyberświecie*

Dzięki udziałowi w projekcie ASCLEPIUS aktywnie wspomagamy sektor ochrony zdrowia w zdobywaniu wiedzy i kompetencji potrzebnych do funkcjonowania w nowoczesnym cyberświecie. Projekt będzie trwał do października 2026 r. i jest przeznaczony dla całej Unii Europejskiej.

Na jakie kwestie związane z cyfrowymi zagrożeniami i cyberbezpieczeństwem położyłby pan szczególny nacisk? Jak zachęcić do zdobywania wiedzy w tym zakresie tych, którzy nie dostrzegają zagrożeń i uważają, że ich to nie dotyczy, że jakoś to będzie?

Ochrona zdrowia doskonale wie, że ciągła edukacja pozwala nie tylko skutecznie leczyć, lecz także zapobiegać chorobom. Dzięki temu procesowi ludzie umieją sobie poradzić w przypadku zwykłego przeziębienia, ale też wiedzą, gdzie się udać po pomoc w cięższych przypadkach. W efekcie społeczeństwo jest zdrowsze, a średnia długość życia ciągle się zwiększa. Podobnie jest z cyberbezpieczeństwem. Wiedzę zdobytą na szkoleniach przenosimy do codziennego życia, dzięki czemu społeczeństwo jest w stanie lepiej identyfikować potencjalne zagrożenia, w szczególności socjotechniczne, które są tak powszechne jak przeziębienia.

Jako osoba borykająca się z otyłością, przez wiele lat ignorowałem tę sprawę, nie dbałem o dietę, bo uważałem, że problem mnie nie dotyczy i że jakoś to będzie. Po rutynowych badaniach krwi okazało się, że mam ogromny problem z tarczycą, a moje organy wewnętrzne były otoczone tłuszczem. Nauczyłem się zdrowiej odżywiać i uprawiać sport. Myślę, że każdy kiedyś zrozumie, że cyberzagrożenia dotyczą nas wszystkich, nawet jeśli nie mamy konta na Facebooku.

Rozmawiał Jacek Janik