**3 pomysły na sprawdzenie wiedzy twoich pracowników o cyberbezpieczeństwie**

* **87% ankietowanych specjalistów IT przyznało, że w ciągu ostatnich trzech lat przeprowadzono skuteczny cyberatak na firmę, w której pracują. Ponadto 83% doświadczyło wzrostu prób ataków – wynika z raportu „2022 Anomali Cybersecurity Insights Report”.**
* **44% ankietowanych wskazało phishing jako najczęściej powtarzającą się formę cyberataków na przestrzeni ostatnich trzech lat.**
* **Hakerzy często próbują atakować również pracowników niższego szczebla, dlatego warto dbać o prawidłowy stan wiedzy na temat cyberzagrożeń wśród wszystkich zatrudnionych.**

Ankietę na temat cyberbezpieczeństwa w czasie pandemii przeprowadzono wśród 800 specjalistów IT z branż finansowej, telekomunikacyjnej i produkcyjnej. To osoby odpowiedzialne za bezpieczeństwo cyfrowe w dużych organizacjach. 87% badanych przyznało, że w ciągu ostatnich trzech lat hakerzy dokonali skutecznego ataku na firmę, w której pracują. Poza tym, 83% respondentów zauważyło wzrost liczby prób cyberataków. Do tego 44% ankietowanych wskazało phishing jako najczęściej powtarzającą się formę ataków hakerskich na przestrzeni ostatnich trzech lat – czytamy w raporcie „2022 Anomali Cybersecurity Insights Report”.

– *Phishing to jedna z najpopularniejszych i nadal skutecznych metod stosowanych przez cyberprzestępców. Hakerzy rozsyłają fałszywe maile lub smsy z linkami lub załącznikami, które po kliknięciu przez ofiarę otwierają przestępcom drogę dostępu do firmowej sieci IT. W ten sposób mogą wykraść dane, pieniądze lub doprowadzić do paraliżu firmowych systemów. Sam phishing może występować także w formie vishingu. Wówczas cyberprzestępcy dzwonią do ofiary i podszywają się pod kogoś z kierownictwa z prośbą o przesłanie konkretnych informacji lub dostępu do wrażliwych danych. Hakerzy stosują social engineering, czyli techniki manipulacyjne i najchętniej atakują szeregowych pracowników organizacji. Zdają sobie sprawę, że poziom wiedzy na temat działań cyberprzestępców może być u nich niższy niż wśród osób zatrudnionych w działach IT –* mówi Patrycja Tatara, ekspert ds. cyberbezpieczeństwa w Sprint S.A.

**Jak sprawdzić wiedzę pracowników na temat cyberzagrożeń?**

Do przeprowadzenia cyberataku hakerzy stosują cały szereg metod, które mogą uśpić czujność u ofiary. Fałszywe wiadomości mogą do złudzenia przypominać np. prawdziwy mail od klienta, gdzie odtworzona jest stopka i język, jakim na co dzień posługuje się kontrahent lub jego branża. Aby zbadać stopień ryzyka powodzenia takiego ataku na twoją organizację, warto sprawdzić poziom świadomości pracowników. Można to zrobić przynajmniej na trzy sposoby.

* **Wyślij „fałszywego” maila**

Najprościej będzie poprosić o przesłanie ważnej informacji lub napisać maila z prośbą o udzielenie dostępu – np. hasła. Wytypuj kogoś z zatrudnionych pracowników, do kogo wyślesz taką wiadomość. Skorzystaj z własnej skrzynki – hakerzy mogą się przecież wcześniej włamać do twojej lub stworzyć adres do złudzenia przypominający ten prawdziwy. W czasie tworzenia treści maila warto napisać go nieco innym językiem, co zdarza się hakerom i jednocześnie da pracownikowi podstawy do wątpliwości. Po wysłaniu wiadomości sprawdź, jak reaguje pracownik – czy np. dzwoni na twój numer służbowy w celu weryfikacji informacji lub pyta cię o otrzymaną wiadomość na wewnętrznym komunikatorze.

* **Napisz SMS z prośbą o hasło**

W podobny sposób czujność pracowników możesz sprawdzić, wysyłając fałszywego SMS-a. Skorzystaj ze służbowego numeru, który posiadają pracownicy twojej organizacji. Pamiętaj, że hakerzy mogą podszyć się pod ten numer, stosując spoofing telefoniczny. W treści wiadomości poproś np. o przesłanie danych dostępowych do którejś z wewnętrznych aplikacji, gdzie w waszej firmie przechowuje się poufne informacje. Następnie, podobnie jak w przypadku maila, obserwuj reakcje pracowników.

* **Zadzwoń do pracownika z prośbą o informację**

W tym celu również nie musisz wykonywać połączenia z innego (np. prywatnego) numeru, z tego samego powodu jak w przypadku wysyłania SMS. W tym celu wybierz pracownika, z którym rzadko masz styczność i jednocześnie pewność, że nie rozpozna cię w mig po głosie. Jeśli jednak prawdopodobieństwo jest duże, inna osoba może zadzwonić z twojego telefonu, podszywając się pod ciebie. Kiedy „ofiara” odbierze połączenie wystarczy zwrócić się do niej z prośbą o udostępnienie poufnej informacji. Następnie obserwuj jej reakcję. Jeśli będzie się wahać, spróbuj ją nakłonić do tego kroku. Pamiętaj, że hakerzy są nieustępliwi.

– *Powyższe metody to skuteczny sposób na zbadanie poziomu wiedzy pracowników na temat cyberzagrożeń. Można podejmować samodzielne próby, ale warto zastanowić się nad zleceniem tego zadania zewnętrznym specjalistom. Oni również stosują symulowane ataki i social engineering, ale ich doświadczenie i umiejętności mogą wykazać jeszcze inne nieprawidłowości w reakcjach pracowników lub ich szersze spectrum. Po drugie, zewnętrzni audytorzy po przeprowadzeniu takich działań przygotują kompleksowy raport i wykażą w nim, co należy zmienić, aby reakcje pracowników były prawidłowe. Kolejne kroki, to przeprowadzenie szkolenia i sprawdzenie nabytych umiejętności w praktyce. Ważne, aby szkolenia pracowników w zakresie cyberbezpieczeństwa były organizowane cyklicznie, bo hakerzy nieustannie doskonalą swoje techniki –* mówi Patrycja Tatara ze Sprint S.A.

Źródło: Sprint S.A.