Eksperci ostrzegają przed wzrostem liczby cyberataków, a Polacy nadal nieświadomi zagrożeń

Kategoria: Styl życia
Opublikowano: piątek, 21, październik 2022 11:44
Alicja Cisowska

Specjaliści CERT odnotowali w Polsce w 2021 r. wzrost cyberataków, aż o 182% w stosunku do roku poprzedniego. Tymczasem, tylko 1/5 badanych Polaków w raporcie Procontent Communication pt. „Polacy w cyberprzestrzeni – Czy jesteśmy świadomi cyberataków?" wskazała, że doświadczyła próby ataku rozumianego jako naruszenie ich Infrastruktury IT w pracy, danych w domowej sieci internetowej lub kradzieży środków finansowych. Wyniki raportu wskazują na poważny problem braku świadomości Polaków w sferze cyberzagrożeń.

Znikoma świadomość społeczeństwa w obliczu cyberataków. Starsze osoby wymagają edukacji.

Statystyki firm zajmujących się badaniem cyberprzestrzeni wskazują na nieustannie zwiększającą się liczbę zgłaszanych incydentów o naruszeniu cyberzabezpieczeń. Zagrożona jest także Polska, która według raportu Check Point Research z czerwca 2022 r. zajmuje szóste miejsce w Europie pod względem zagrożeń cybernetycznych. Polacy nie zdają sobie jednak sprawy z wagi problemu. Aż 82% badanych deklaruje, iż nie doświadczyło próby cyberataku osobiście, a świadomość zagrożeń spada wraz z wiekiem. 22% osób do 24 roku życia wskazało, że zetknęło się z próbą ataku, podczas gdy w grupie wiekowej osób powyżej 50 roku życia twierdząco odpowiedziało tylko 14% badanych. Raport jasno wskazuje zatem grupy wiekowe, na które warto zwrócić szczególną uwagę w kwestii edukacji nt. podstawowych zasad cyberbezpieczeństwa oraz rozpoznawania cyberataków.

Szczególne zagrożenie dla firm.

Dane Check Point Research wskazują, że w pierwszej połowie 2022 r. nastąpił 42% wzrost tygodniowych cyberataków w skali globalnej, przy czym każdy kontynent doświadczył znacznej eskalacji. Według ekspertów w dziedzinie cyberbezpieczeństwa na cyberataki najbardziej narażone są infrastruktury IT firm, ze względu na większą wartość wykradanych danych. W Europie występuje średnio tysiąc ataków tygodniowo na jedną organizację. To wzrost o 26% w porównaniu z rokiem poprzednim. Pracodawcy, bagatelizując komunikację dotyczącą bezpieczeństwa informacji, przyczyniają się do niewiedzy pracowników. Jednakże, żeby móc przeciwdziałać problemowi, najpierw trzeba zrozumieć jego istotę. Propagowanie podstawowej wiedzy dotyczącej najprostszych zagadnień z branży IT może okazać się pomocne, szczególnie jeśli mowa o zapobieganiu zyskującym na popularności metodom oszustw i ataków w cyberprzestrzeni.

- Cyberbezpieczeństwo staje się istotnym tematem w debacie publicznej. Wzmożone ataki hakerów mające miejsce od rozpoczęcia wojny w Ukrainie oraz przyśpieszona cyfryzacja gospodarki związana z pandemią COVID-19 spowodowały wzrost zainteresowania kwestią zagrożeń w cyberprzestrzeni. Polacy słusznie dostrzegli, iż od czasu napaści zbrojnej na Ukrainę zwiększyła się m.in. liczba cyberataków na polską infrastrukturę IT. Przeprowadzony przez nas raport wskazał jednak na znikomą wiedzę Polaków w kwestii dostrzegania cyberataków we własnym otoczeniu. Wyniki jasno pokazują, iż trzeba położyć nacisk na edukację praktycznie całego społeczeństwa, gdyż ponad 80% z nas nie zdaje sobie sprawy, że każdego dnia może być bezpośrednim celem ataków. Jednocześnie, zdaniem badanych, wiele firm nadal nie wdrożyło odpowiednich procedur bezpieczeństwa i nie edukuje pracowników w zakresie rozpoznawania cyberataków. - mówi Iwona Kubicz, Prezes Procontent Communication.

Co więcej, z raportu wynika, że bardziej świadomi cyberzagrożeń są mieszkańcy wsi niż większych miast. Blisko co piąty badany z obszarów wiejskich przyznaje, iż doświadczył w ostatnim roku próby napaści na infrastrukturę IT, natomiast w miastach (powyżej 500 tys. mieszkańców) takich wskazań było zaledwie 12%. Inwestycje w odpowiednią edukację powinny być zatem priorytetem zarówno w

obszarach o większym zaludnieniu, jak również w mniejszych miejscowościach.

Wojna w Ukrainie. Cyberataki na niespotykaną dotąd skalę.

Raport ESET Threat Report z czerwca 2022 r. potwierdza fakt, iż wojna w Ukrainie poskutkowała zwiększeniem liczby zagrożeń w cyberprzestrzeni. Polska, będąc członkiem NATO oraz ze względu na swoje położenie geograficzne jest na nie szczególnie narażona. Jak wynika z raportu Procontent, Polacy są świadomi wzrostu zagrożenia – ponad 58% badanych łączy zwiększenie liczby ataków z wybuchem wojny w Ukrainie. Tylko niewielki procent badanych (18%) ma jednak poczucie, że zagrożenia mogą dotyczyć bezpośrednio ich samych. W tym przypadku większą wiedzą wykazują się osoby z wyższym wykształceniem.

Skuteczne działania komunikacyjne oraz przygotowanie zaawansowanych cyberzabezpieczeń to podstawa. Firmy powinny śledzić rozwój w tym obszarze, by móc przeciwdziałać ewentualnym kryzysom, a w razie ataku, zareagować w odpowiednim tempie. Opinia publiczna powinna natomiast być informowana, o nowych rodzajach zagrożeń i ich społecznym oddziaływaniu. IPR (Institute for Public Relations) zwraca uwagę na istotę edukacji pracowników w firmie w postaci budowania tzw. kultury świadomości cyberbezpieczeństwa. Stowarzyszenie sugeruje, by zwrócić szczególną uwagę na znajomość przez pracowników obowiązujących w firmie zasad dotyczących bezpieczeństwa danych oraz przepisów odnoszących się do funkcjonowania w cyberprzestrzeni.

- Sektor cyberbezpieczeństwa rozwija się w zawrotnym tempie, jednak infrastruktura i zabezpieczenia to nie wszystko, bardzo ważny jest również czynnik ludzki. Tu konieczna jest edukacja i monitoring reakcji pracowników na zagrożenia. Ważne jest także budowanie wagi cyberbezpieczeństwa w firmach i podkreślanie ich roli w funkcjonowaniu organizacji. W tym celu istotne jest, nie tylko prowadzenie projektów komunikacyjnych w zakresie wykrywania i reagowania na cyberzagrożenia, ale także wprowadzanie członków zespołów ds. cyberbezpieczeństwa do procesów planowania projektów marketingowych, komunikacji wewnętrznej i wydarzeń firmowych. Jednym z trendów w komunikacji na świecie jest budowanie większego zaangażowania zespołów ds. cyberbezpieczeństwa w realizowane przez firmy projekty – podkreśla Iwona Kubicz.

Raport powstał w wyniku pracy zespołu Procontent Communication oraz SW Research. Całość niebawem ukaże się w kanałach mediowych agencji, między innymi na www.procontent.pl

Źródło: IP