Kontakt dla mediów:
Luiza Nowicka, PARP
e-mail: luiza_nowicka@parp.gov.pl
tel.: 880 524 959

Informacja prasowa
Warszawa, 30.03.2022 r.

Biznes bezpieczny w sieci. Jak zadbać o cyberbezpieczeństwo?

Firmy w coraz większym stopniu wykorzystują możliwości, jakie daje Internet, narzędzia do zdalnej pracy i komunikacji czy te pozwalające na elektroniczny obieg dokumentów i przechowywanie danych w formie cyfrowej. A cyberprzestępcy nie śpią. Średnio nawet co 11 sekund może dochodzić do cyberataku.

Phishing, spoofing, ataki z użyciem szkodliwego oprogramowania, kradzież danych czy blokowanie dostępu do usług – to tylko niektóre z zagrożeń w cyberprzestrzeni, na które narażeni są nie tylko indywidualni użytkownicy, ale także przedsiębiorcy. A coraz więcej z nich – zwłaszcza od wybuchu pandemii COVID-19 – jest obecnych w sieci. Za jej pomocą łączy się z pracownikami i kontrahentami czy sprzedaje swoje produkty i usługi.

Rok 2020 pokazał, że przedsiębiorstwa muszą być przygotowane na szybkie podejmowanie decyzji. Umiejętność dostosowania się do zmieniającej się rzeczywistości, pozwoliła wielu z nich przetrwać pandemię i związane z nią lockdowny. Niektórzy dzięki zastosowaniu narzędzi informatycznych, w okresie obostrzeń związanych z COVID-19, przebili się na rynku i zwiększyli swoje zasięgi.

Pandemia przyniosła też kolosalną zmianę na rynku pracy. Wielu pracowników swoje obowiązki zawodowe wykonuje zdalnie. Wcześniej przedsiębiorcy podchodzili do tego rozwiązania z rezerwą. Według badań zawartych w raporcie PARP „Aspekty pracy zdalnej z perspektywy pracownika, pracodawcy i gospodarki", po wybuchu pandemii COVID-19, odsetek pracodawców nastawionych negatywnie do wykonywania obowiązków zawodowych z domu zmalał z 27,6% do 11,7%. Aż 92% przedsiębiorców zadeklarowało, że efektywność pracy zdalnej jest dobra lub bardzo dobra. Wszystko wskazuje na to, że także po ustabilizowaniu się sytuacji epidemicznej, przedsiębiorcy będą w większym stopniu niż wcześniej korzystać z pracy zdalnej.

Wzrastająca skala zagrożenia cyberatakami i realne straty dla firm

Przeniesienie pracy i aktywności gospodarczej do sieci zaktywizowało cyberprzestępców.

– Z początkiem pandemii znacznie wzrosła liczba zagrożeń w Internecie. Przedsiębiorcy musieli zmierzyć się z coraz liczniejszymi atakami z najróżniejszych zakątków świata – zwraca uwagę **Robert Muchacki**, zastępca dyrektora PARP ds. Bezpieczeństwa Informatycznego – Obecna

sytuacja na Wschodzie pokazała jak ważna jest rola cyberbezpieczeństwa. Specjaliści zaobserwowali zwiększoną liczbę ataków także na przedsiębiorców – podkreśla.

Wykorzystywanie cyberataków w polityce międzynarodowej czy w walce o dominację gospodarczą to nic nowego. Pierwszą bronią cyfrową nazwano wykryty w 2010 r. wirus Stuxnet. Wiele wskazuje na to, że został stworzony przez wywiady USA oraz Izraela i skutecznie opóźnił rozwój irańskiego programu atomowego poprzez uszkodzenie urządzeń wykorzystywanych przez irańskich naukowców.

Z raportu firmy Check Point Research wynika, że przedsiębiorstwa są stale narażone na zagrożenia cybernetyczne. W czwartym kwartale 2021 r. zanotowano najwyższy w historii cotygodniowy szczyt cyberataków na organizacje, ponad 900 tygodniowo. W 2021 r. nastąpił 50-procentowy wzrost ogólnej liczby ataków tygodniowo w sieciach korporacyjnych w porównaniu z 2020 r. Najwięcej ataków w 2021 r. doświadczyła branża edukacyjna i badawcza, średnio 1605 ataków na organizację tygodniowo. Kolejny był sektor rządowy i wojskowy z liczbą 1136 ataków i 47- procentowym wzrostem względem 2020 r. W Europie odnotowano 68-procentowy tygodniowy wzrost cyberataków, porównując 2020 i 2021 r. Cybersecurity Ventures przewidywało, że w 2021 r. firmy mogły być przedmiotem cyberataku co 11 sekund. Wskazują też, że ponad 50% wszystkich cyberataków dotyczy małych i średnich firm, a 60% z nich wypada z działalności w ciągu sześciu miesięcy od padania ofiarą naruszenia bezpieczeństwa danych lub włamania. Cyfrowe ataki przekładają się na całkiem realne straty. W samym 2021 r. wartość wykradzionych danych personalnych przekroczyła 4,24 mln dolarów (źródło: Cost of a Data Breach Report 2021).

Najczęstszymi atakami w 2021 r. były próby wykradzenia danych przez e-mail, szyfrowanie plików w zamian za wynagrodzenie, wykorzystywanie szkodliwego oprogramowania, ujawnienie danych firmowych czy ataki uniemożliwiające korzystanie z infrastruktury.

Unia Europejska z *Cybersecurity Act*

Coraz częściej cyberataki mają charakter ponadnarodowy i swoim zasięgiem obejmują teren więcej niż jednego państwa. „Przykładem takich zdarzeń może być atak z użyciem złośliwego oprogramowania WannaCry, który miał miejsce w maju 2017 r. i doprowadził do zainfekowania kilkuset tysięcy komputerów w około 100 państwach. Skutkiem ataku było m.in. sparaliżowanie brytyjskiej służby zdrowia czy też utrudnienie działalności jednego z hiszpańskich operatorów telekomunikacyjnych” – przypominał w 2019 r. w analizie dla „Biuletynu Euro Info” radca prawny Michał Nosowski, specjalizujący się w problematyce prawa nowych technologii oraz ochronie danych osobowych. Zwracał również uwagę, że Unia Europejska w obliczu zagrożenia cyberatakami wykazała zwiększoną aktywność w zakresie tworzenia prawa, odnoszącego się do kwestii cyberbezpieczeństwa. Przyjęła m.in. *Cybersecurity Act* mający na celu podniesienie poziomu bezpieczeństwa IT na terenie UE. Stosowany jest on bezpośrednio, bez konieczności implementacji jego postanowień przez państwa członkowskie.

Wcześniej, bo już w 2018 r., Polska implementowała unijną dyrektywę NIS w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych. Na mocy tych przepisów ustanowiony został system, który ma za zadanie zapewnienie cyberbezpieczeństwa na poziomie krajowym. Przepisy do zadbania o cyberbezpieczeństwo zobowiązały także przedsiębiorców z grupy tzw. operatorów usług kluczowych. Należą do niej firmy z sektora energii, transportu, infrastruktury cyfrowej, bankowości i infrastruktury rynków finansowych, ochrony zdrowia czy zaopatrzenia w wodę pitną.

Zainwestuj w cyberbezpieczeństwo

Cyberbezpieczeństwo ma kolosalne znaczenie nie tylko dla firm dostarczających usługi i towary o znaczeniu strategicznym, ale również dla małych i średnich przedsiębiorstw wszystkich branż. – Badania pokazują, że okres pandemii i związana z nią konieczność przeniesienia części działalności do sieci, skłoniła wiele firm do zwrócenia uwagi na kwestie cyberbezpieczeństwa. Inwestuje w nie coraz więcej firm z sektora MŚP. Stosują środki bezpieczeństwa ICT, przyjmują strategię bezpieczeństwa teleinformatycznego i zwracają uwagę na poziom wyszkolenia kadry – mówi Robert Muchacki, zastępca dyrektora PARP ds. Bezpieczeństwa Informatycznego.

Z „Raportu o stanie sektora małych i średnich przedsiębiorstw w Polsce 2021" przygotowanego przez PARP wynika, że w 2020 r. 95% przedsiębiorstw zastosowało środki bezpieczeństwa teleinformatycznego. Wśród nich były: bieżąca aktualizacja oprogramowania (83,1% wskazań), wykonywanie zapasowych kopii danych i przekazywanie ich do innych lokalizacji (61,3%), uwierzytelnianie silnym hasłem (8%), identyfikacja i uwierzytelnianie metodami biometrycznymi (7,1%). 28,4% spośród badanych przedsiębiorców przeprowadziło w 2020 r. audyt bezpieczeństwa swojego systemu informacyjnego.

Jakie zadbać o bezpieczeństwo teleinformatyczne w firmie? Wskazujemy trzy podstawowe kroki.

1. **Wiedza**

Jednym z najważniejszych aspektów cyberbezpieczeństwa jest stałe podnoszenie świadomości wśród pracowników firmy. Regularne szkolenia i przypominanie zasad bezpieczeństwa, to podstawa do skutecznej ochrony przed zagrożeniami z zewnątrz. Atak cybernetyczny może zostać wykryty przez zastosowane w firmie systemy, ale trzeba pamiętać, że atakujący stale się rozwijają, wymyślają nowe metody, poprawiają swój warsztat, by wymknąć się narzędziom monitorującym bezpieczeństwo naszej sieci i baz danych. Na końcu zawsze jest człowiek. Warto, by wiedział, jak zareagować w danej sytuacji.

W podnoszeniu kwalifikacji pracowników firmy pomocne są m.in. materiały edukacyjne na platformach wideo czy certyfikowane szkolenia przygotowywane przez profesjonalnych organizatorów. Swoją ofertę dla przedsiębiorców ma także PARP. W ramach Akademii PARP proponujemy pięciogodzinny kurs online prowadzony przez eksperta w dziedzinie cyberbezpieczeństwa. Interesujące szkolenia w tej dziedzinie można też łatwo znaleźć w prowadzonej przez PARP Bazie Usług Rozwojowych (BUR).

– Przedsiębiorcy są coraz bardziej świadomi tego, jak ważne dla ich biznesów jest cyberbezpieczeństwo: poszukują wiedzy, porad ekspertów, ale również firm świadczących usługi w tym obszarze. Polska Agencja Rozwoju Przedsiębiorczości wychodząc naprzeciw tym oczekiwaniom, przygotowała szkolenia i kursy on-line, do korzystania z których zachęcamy przedsiębiorców – mówi prezes PARP **Dariusz Budrowski**. Dodaje, że dużym zainteresowaniem cieszy się szkolenie Akademii PARP „Cyberbezpieczeństwo w MŚP", na które zapisało się już ponad 2,5 tys. osób, a tygodniowo przybywa około 40 nowych zapisów. – Dostępne w Bazie Usług Rozwojowych szkolenia z zakresu bezpieczeństwa IT cieszą się równie dużą popularnością. Prawie 3,1 tys. osób zapisało się na usługi z tej podkategorii, przy czym ponad 2,8 tysiąca już je ukończyło. Co ważne, szkolenia oferowane w BUR skierowane są zarówno dla uczestników posiadających dofinansowanie ze środków publicznych, jak i tych, którzy koszty pokrywają z własnych środków – wyjaśnia prezes PARP.

2. Dobre praktyki

Nie da się ukryć, że najlepszym zabezpieczeniem przedsiębiorstwa jest właściwe postępowanie w odniesieniu do potencjalnych zagrożeń cybernetycznych. Do dobrych praktyk należą regularne szkolenia personelu, wewnętrzne procedury reagowania na potencjalne zagrożenia, jak i współpraca pomiędzy firmami. Skutecznym narzędziem walki z atakami cybernetycznymi jest stosowanie wspólnych zespołów typu SOC (ang. *Security Operations Center* – Centra Operacji Bezpieczeństwa). Centra te są oparte o nowoczesne technologie oraz procedury bezpieczeństwa. Skupiają ludzi odpowiedzialnych za szybkie wykrywanie zagrożeń. W ramach zespołów SOC danej branży, poszczególni uczestnicy mogą wymieniać się wiedzą, spostrzeżeniami. Łatwiej też jest wychwycić atak kierowany na daną branżę – np. w firmy związane z sektorem finansowym czy szkoleniowym.

3. Doświadczony personel

By zabezpieczyć firmę przed atakami cyberprzestępców, potrzebne będzie wsparcie fachowców. Choć cyberbezpieczeństwo jest bezsprzecznie dziedziną przyszłości, to wciąż brakuje specjalistów z tego obszaru. Możemy wręcz mówić o przepaści między potrzebami rynku, a dostępnością specjalistów. Szacuje się, że potrzebnych jest 3,5 mln takich pracowników. Liczba nieobsadzonych stanowisk w zakresie cyberbezpieczeństwa wzrosła o 350%, z miliona stanowisk w 2013 r. do 3,5 miliona w 2021 r. (źródło: Cybercrime Magazine, 2022 Cybersecurity Almanac).

Trudności z rekrutacją specjalistów do działów cyberbezpieczeństwa sprawiły, że popularnym rozwiązaniem w tym obszarze są usługi B2B. Przedsiębiorstwo wyspecjalizowane w świadczeniu usług związanych z bezpieczeństwem informatycznym, oferuje je innym firmom. A w Polsce przybywa tych, którzy świadczą tego typu usługi. Wiele z nich rozwija się dzięki dotacjom z PARP, pochodzącym z Funduszy Europejskich. Wśród wspartych biznesów znalazła się firma ICsec, która oferuje rozwiązania z zakresu cyberbezpieczeństwa infrastruktury przemysłowej. Z kolei Sagenso świadczy usługi zabezpieczania danych i umożliwia monitorowanie zagrożeń cybernetycznych w trybie 24/7. Specfile Projects jest autorem aplikacji szyfrującej, dzięki której można zabezpieczyć

obieg dokumentów w firmie. Firmy te uzyskały wsparcie w ramach programów dla start-upów, takich jak Scale Up oraz Programów Akceleracyjnych łączących początkujących, kreatywnych przedsiębiorców z infrastrukturą oraz doświadczeniem dużych przedsiębiorstw. Oba finansowane są w ramach Programu Operacyjnego Inteligentny Rozwój (POIR).

Więcej o firmach z branży bezpieczeństwa teleinformatycznego, które rozwijają się dzięki wsparciu z Funduszy europejskich przekazywanych przez PARP przeczytasz w drugim odcinku naszego cyklu „Cyberbezpieczeństwo”.