Cyfrowe niebezpieczeństwo: Chroń swoją firmę przed nowymi zagrożeniami już teraz!

Rok 2024 przynosi nowe wyzwania w świecie cyberbezpieczeństwa. Cyfrowy ekosystem staje się coraz bardziej niebezpieczny, a każdy dzień pokazuje, że zarówno małe, jak i duże firmy są narażone na cyberataki. Według Cybersecurity Ventures, koszty globalnej cyberprzestępczości mają osiągnąć do 2025 roku 10,5 biliona dolarów. Czego możemy nauczyć się z ostatnich cyberataków i jak się przed nimi chronić?

Cyberataków coraz więcej: liczba wzrosła pięciokrotnie

Ostatnie lata przyniosły falę cyberataków, które wstrząsnęły światem biznesu i technologii. Incydenty w kwestii cyberbezpieczeństwa uwidoczniły słabości nawet najbardziej zaawansowanych infrastruktur IT. Te wydarzenia nie tylko uświadomiły firmom konieczność inwestowania w cyberbezpieczeństwo, ale także dostarczyły cennych lekcji na temat zagrożeń, jakie czyhają w cyfrowym świecie. Analizując te przypadki, możemy lepiej zrozumieć, jakie błędy zostały popełnione i jakie środki zapobiegawcze mogą pomóc w uniknięciu podobnych sytuacji w przyszłości.

W maju 2024 roku liczba cyberataków na polskie firmy wzrosła pięciokrotnie w porównaniu z poprzednim rokiem, jak podają najnowsze dane ESET. Pierwszy kwartał 2024 roku przyniósł Polakom ostrzeżenie Komisji Nadzoru Finansowego o oszustach podszywających się pod Bank Millennium, którzy promowali fałszywe ankiety na mediach społecznościowych. Po ich wypełnieniu użytkownicy mieli otrzymać pieniądze, jednak w rzeczywistości oszuści wyłudzali dane osobowe oraz informacje o kartach płatniczych.

W tym samym czasie, w Niemczech, urząd miasta Fürth padł ofiarą ataku DDoS, który zablokował wszystkie strony urzędu. Podobny incydent miał miejsce we Francji w gminie Chalosse Tursan w departamencie Landes, gdzie cyberatak zakłócił systemy informatyczne, co znacznie utrudniło funkcjonowanie usług publicznych.

W Belgii z kolei, w marcu 2024 roku, produkcja we wszystkich browarach Duvel Moortgat, została zatrzymana ze względu na cyberatak. Incydent, przypisywany grupie rosyjskich hakerów, uruchomił system bezpieczeństwa browaru, który wyłączył serwery w celu ochrony przed dalszymi szkodami.

Ataki phishingowe

Phishing jest obecnie najpopularniejszym narzędziem cyberprzestępców. To technika oszustwa internetowego, w której cyberprzestępcy podszywają się pod zaufane osoby lub instytucje, aby wyłudzić poufne dane, takie jak hasła czy informacje bankowe, poprzez fałszywe wiadomości e-mail, strony internetowe lub wiadomości tekstowe. Według raportu Lookout, połowa posiadaczy smartfonów była celem ataków phishingowych każdego kwartału 2022 roku. W styczniu 2023 roku firma Reddit ogłosiła, że ich pracownicy padli ofiarą zaawansowanego ataku phishingowego, w wyniku którego doszło do

wycieku danych pracowników i kodów dostępowych. Edukacja i regularne szkolenia pracowników są kluczowe, aby sprostać temu zagrożeniu.

Złośliwe oprogramowanie

Przez ostatnie lata odnotowano również znaczny wzrost ataków malware (złośliwego oprogramowania), czyli oprogramowania stworzonego w celu infiltracji, uszkodzenia lub uzyskania nieautoryzowanego dostępu do systemów komputerowych, sieci lub danych użytkownika, obejmującego wirusy, trojany, ransomware i spyware. W lutym 2023 roku, Orange Spain doświadczyła poważnej awarii po tym, jak aktor zidentyfikowany jako "Snow" uzyskał dostęp do konta zarządzającego globalną tablicą routingu przy użyciu "niedorzecznie słabego" hasła. Infostealing malware zainfekował komputer administratora, kradnąc hasło, które następnie sprzedano na dark webie. Snow wykorzystał to do logowania do konta Orange w RIPE NCC, co doprowadziło do manipulacji tablicą routingu i w końcu do ataku typu denial of service.

Nauka na cudzych błędach

W obliczu rosnącej liczby cyberataków, wdrożenie codziennych praktyk z zakresu cyberbezpieczeństwa staje się niezbędnym elementem funkcjonowania każdej firmy. Dobre praktyki, takie jak regularne aktualizacje oprogramowania, stosowanie silnych haseł czy przeprowadzanie szkoleń dla pracowników, mogą znacząco zmniejszyć ryzyko naruszenia bezpieczeństwa danych. O 5 kwestiach, o których należy pamiętać, aby uchronić Twoją firmę przed potencjalnymi cyberatakami, opowiada **Michał Billewicz, Senior Compliance Officer w Britenet.**

- **Szkolenia pracowników** – Edukacja pracowników w zakresie rozpoznawania prób phishingu, używania silnych haseł i bezpiecznego korzystania z internetu jest kluczowa dla ochrony firmy. Regularne szkolenia i symulacje phishingowe mogą pomóc w zbudowaniu świadomości wśród pracowników.

- **Dwuskładnikowe uwierzytelnianie (2FA)** – Zastosowanie dwuskładnikowego uwierzytelniania znacząco utrudnia dostęp do systemów i danych przez niepowołane osoby. 2FA wymaga drugiego składnika uwierzytelniania, takiego jak kod SMS, aplikacja mobilna, token sprzętowy lub biometryka, co zwiększa poziom zabezpieczeń.

- **Szyfrowanie danych i kopie zapasowe** – Szyfrowanie to zabezpieczenie, które sprawia, że nawet jeśli dane zostaną skradzione, będą bezużyteczne bez odpowiedniego klucza. Szyfrowanie powinno być stosowane zarówno podczas przesyłania danych, jak i w spoczynku. Regularne tworzenie kopii zapasowych danych jest kluczowe w przypadku ataków, takich jak ransomware.

- **Regularne aktualizacje** – Systemy i oprogramowanie powinny być regularnie aktualizowane, aby zapobiec znanym lukom w zabezpieczeniach. Regularne aktualizacje pomagają w utrzymaniu wysokiego poziomu ochrony przed nowymi zagrożeniami, które pojawiają się każdego dnia. Pracownicy IT powinni monitorować dostępność poprawek i aktualizacji oraz wdrażać je jak najszybciej, aby minimalizować ryzyko potencjalnych ataków.

- **Monitorowanie i wykrywanie zagrożeń** – Aktywne monitorowanie systemów IT w czasie rzeczywistym oraz wdrażanie systemów do wykrywania i reagowania na zagrożenia może znacząco wpłynąć na szybkość reakcji na incydenty, a także ułatwić ich obsługę.

Zabezpiecz swoją firmę na przyszłość

Cyberbezpieczeństwo to dziedzina, która z każdym rokiem nabiera coraz większego znaczenia. Ostatnie incydenty uświadomiły nam, jak ważne jest nie tylko posiadanie odpowiednich technologii ochronnych, ale również stałe doskonalenie procedur bezpieczeństwa i podnoszenie świadomości pracowników. W świecie pełnym nieustannie ewoluujących zagrożeń cybernetycznych, firmy muszą być zawsze czujne i świadome ryzyka. Podane powyżej przykłady mechanizmy ochrony to minimalne elementy ochrony, właściwe dla każdej organizacji, niezależnie od sektora, w którym działa. Pomóc może w tym również dobry partner IT, taki jak Britenet, który pomoże Ci zadbać o cyberbezpieczeństwo w Twojej firmie.

O Britenet

Britenet to firma specjalizująca się w rozwoju oprogramowania, lider w branży technologicznej, oferujący innowacyjne rozwiązania dla klientów na całym świecie. Firma została założona w 2006 roku i od tego czasu dynamicznie się rozwija, zdobywając uznanie na rynkach lokalnych i międzynarodowych. Misją Britenet jest wdrażanie transformacji cyfrowej u swoich partnerów oraz dostarczanie najwyższej jakości produktów i usług, które zmieniają sposób życia i pracy klientów. Britenet zdobył zaufanie ponad 200 międzynarodowych klientów z różnych branż, w tym polskich i zagranicznych firm reprezentujących takie sektory, jak finanse, bankowość, edukacja, energetyka i ubezpieczenia.

Kontakt dla mediów:

Małgorzata Garnek-Dudek
PR & Communication Leader
+48 539 016 451
malgorzata.garnek-dudek@britenet.eu