Bitdefender

# Wyzwania związane z cyberbezpieczeństwem, przed którymi stoją firmy w 2023 roku

12.04.2023

Zespół Bitdefender niedawno opublikował coroczny raport dotyczący cyberzagrożeń, który przedstawia aktualne trendy i potrzeby zespołów do spraw cyberbezpieczeństwa. Działy te muszą nie tylko radzić sobie ze wzrostem liczby incydentów typu ransomware, phishing i ataków na łańcuchy dostaw, ale są również zmuszone do zmagania się ze złożonymi środowiskami, ponieważ organizacje coraz bardziej polegają na chmurze hybrydowej i aplikacjach SaaS.

Niestety zespół Bitdefender zauważa, że coraz częściej złożoność środowiskowa przytłacza działy cyberbezpieczeństwa, które już teraz mają trudności ze znalezieniem odpowiednich zasobów do zapewnienia swojej firmie odpowiedniego poziomu cyberochrony. Niektóre przedsiębiorstwa obecny kryzys gospodarczy doprowadził do zminimalizowania budżetów i – co za tym idzie – wyzwań związanych z

zatrudnieniem specjalistów do spraw cyberbezpieczeństwa, podczas gdy inne są przeciążone zbyt dużą liczbą dostawców, narzędzi i źródeł danych. W rezultacie ponad połowa organizacji ucierpiała w wyniku naruszenia bezpieczeństwa danych w ciągu ostatnich 12 miesięcy — a większość z nich została poproszona o utrzymanie wycieku danych w tajemnicy pomimo potencjalnych konsekwencji.

Bitdefender przeprowadził ankietę wśród 400 specjalistów IT na całym świecie, od menedżerów IT po CISO, z różnych sektorów przemysłu pracujących w organizacjach zatrudniających ponad 1000 pracowników, aby odkryć największe wyzwania związane z cyberbezpieczeństwem firm w 2023 roku. Poniżej przedstawiamy wyniki przeprowadzonych badań.

## Wyzwania związane z cyberbezpieczeństwem firm w 2023 roku

Tak jak infrastruktura organizacji ewoluuje, aby sprostać zmieniającym się potrzebom biznesowym, tak samo ewoluują zestawy narzędzi wykorzystywane przez hakerów do uzyskiwania wrażliwych danych. Coraz częściej wykorzystują oni wirusy z rodziny ransomware, stosując taktykę podwójnego wymuszenia, w ramach której oprócz szyfrowania kradną i eksfiltrują dane swoich ofiar. Podobnie techniki inżynierii społecznej ewoluują do tego stopnia, że ataki phishingowe stają się coraz bardziej przekonujące.

Nic dziwnego, że prawie wszyscy (99%) specjaliści do spraw

cyberbezpieczeństwa są zaniepokojeni tymi zmieniającymi się zagrożeniami. Wyniki ankiety przeprowadzonej przez zespół Bitdefender pokazują, że luki w zabezpieczeniach i exploity zero-day pozostają głównymi problemami zespołów IT, tuż za nimi plasują się ataki na łańcuchy dostaw, oprogramowanie ransomware i ataki socjotechniczne. Ponad 72% ankietowanych stwierdziło, że ich firmy odnotowały wzrost wyrafinowania ataków phishingowych.

Obawy specjalistów są uzasadnione, ponieważ ponad połowa (52%) respondentów stwierdziła, że w ciągu ostatnich 12 miesięcy doświadczyła naruszenia danych w wyniku incydentu związanego z cyberbezpieczeństwem. Wyciek danych odnotowało aż 75% respondentów ze Stanów Zjednoczonych, 51% z Wielkiej Brytanii, 49% z Niemczech i 42% z Francji.

Wiele organizacji, których to dotyczy, twierdzi, że powiedziano im, aby zachowały poufność wycieku danych, mimo że mają obowiązek go zgłosić. Ponad 40% ankietowanych specjalistów ds. bezpieczeństwa stwierdziło, że nakazano im, aby utrzymywali włamanie w tajemnicy; wśród respondentów z USA było to 71%. Dla porównania, tylko 15% respondentów w Niemczech i 27% we Francji zachowało informacje o naruszeniu danych w tajemnicy, chociaż wiedziało, że należy je zgłosić.

## XDR – jak może pomóc?

Liderzy bezpieczeństwa zmagają się z rosnącą liczbą potencjalnych zagrożeń. Wielu z nich ma również do czynienia ze skutkami narażenia

na szwank przez hakerów i ich ewoluujące zestawy narzędzi.

Ponad 40% ankietowanych specjalistów oświadczyło, że nie jest w stanie rozszerzyć możliwości w wielu środowiskach. Inni twierdzili, że przeszkadza im złożoność, zbyt wiele alertów i brakuje im umiejętności w zakresie bezpieczeństwa, aby osiągnąć optymalny poziom cyberochrony. Zaledwie 2,6% respondentów nie napotkało żadnych problemów z obecnym rozwiązaniem, a ponad połowa stwierdziła, że ich organizacja kupiła narzędzie bezpieczeństwa, które nie spełniło oczekiwań.

Na szczęście większość liderów IT (74% respondentów) twierdzi, że pomimo obecnego kryzysu gospodarczego, który spowodował masowe zwolnienia i zmniejszenie wydatków, planują zwiększyć swoje budżety na bezpieczeństwo w 2023 roku. Liczba ta wynosi ponad 78% wśród respondentów w USA i około 70% wśród europejskich przedsiębiorstw. Podobnie trzy czwarte liderów bezpieczeństwa w skali globalnej twierdzi, że w 2023 roku planuje wprowadzić więcej rozwiązań antywirusowych.

## Czego firmy oczekują od rozwiązań antywirusowych w 2023 roku?

Niemal wszyscy (93%) respondenci stwierdzili, że proaktywne podejście do cyberzagrożeń jest konieczne, a jeszcze większa liczba zadeklarowała potrzebę całodobowej ochrony. Rozwiązania XDR spełniają powyższe potrzeby. XDR nie tylko wyposaża organizacje w całodobowe monitorowanie bezpieczeństwa, zaawansowane

zapobieganie atakom, wykrywanie i usuwanie zagrożeń, lecz także zapewnia automatyczną korelację danych wielu warstw, między innymi poczty elektronicznej, serwerów, punktów końcowych i danych w chmurze.

Ankietowani liderzy byli również pewni, że konieczna jest zmiana sposobu myślenia z „za cyberbezpieczeństwo odpowiada dział IT" na „za cyberbezpieczeństwo odpowiadają wszyscy pracownicy". Zwiększenie świadomości bezpieczeństwa w celu uwzględnienia szerokiego zakresu ataków jest koniecznością, zwłaszcza że zagrożenia, które codziennie trafiają na pierwsze strony gazet, często wykorzystują ludzkie słabości i przeoczone luki w zabezpieczeniach.

„Dane zgromadzone przez zespół Bitdefender pokazują, że aż 95% naruszeń bezpieczeństwa danych jest efektem prostych ludzkich błędów. Dlatego podstawowym problem, na którym powinny się skupić firmy i instytucje to odpowiednia edukacja pracowników w zakresie podstawowych zasad cyberbezpieczeństwa" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

## Ocena cyberbezpieczeństwa w 2023 roku

Ocena bezpieczeństwa cybernetycznego Bitdefender na rok 2023 stanowi doskonałe przypomnienie o stałych zagrożeniach, z którymi obecnie borykają się lokalne, chmurowe i hybrydowe środowiska bezpieczeństwa i o tych, które będą im towarzyszyć w nadchodzących

latach.

„Wyniki tego raportu ukazują organizacje znajdujące się pod ogromną presją. Muszą one stawić czoła ewoluującym zagrożeniom, takim jak oprogramowanie ransomware, luki dnia zerowego i szpiegostwo, jednocześnie zmagając się ze złożonością rozszerzania ochrony bezpieczeństwa na różne środowiska i ciągłym niedoborem umiejętności” — powiedział Andrei Florescu, zastępca generalnego menedżera i starszy wiceprezes produktów w Bitdefender Business Solutions Group.

Źródło:https://bitdefender.pl/wyzwania-zwiazane-z-cyberbezpieczenstwem-przed-ktorymi-stoja-firmy-w-2023-roku/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 12.04.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej

innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.