GRANDMETRIC
STAY CONNECTED.

cisco Partner

Cyfrowe bezpieczeństwo fabryk

Kluczowe wnioski z raportu przygotowanego przez Grandmetric i Computerworld



Zabezpieczeni, ale czy na pewno bezpieczni?



Pandemia COVID-19 zmieniła krajobraz biznesowy. W rezultacie wiele firm z sektora produkcji stanęło przed **ogromnymi wyzwaniami związanymi z koniecznością podjęcia nowych inwestycji w infrastrukturę oraz zwiększenia poziomu zabezpieczeń**.

Grandmetric przeprowadził badanie, które miało na celu znalezienie odpowiedzi na pytanie, czy w ostatnim roku firmy z sektora wytwórczego i dystrybucji potrafiły dostosować swoją infrastrukturę do zmieniającego się otoczenia?

W poniższym materiale prezentujemy najważniejsze wnioski z raportu, dotyczące zagadnień związanych z **podejściem do cyberbezpieczeństwa**.

Choć liczba cyberataków w pandemii wzrosła 4-krotnie*, **zaledwie 20% firm produkcyjnych wzmocniło swoje narzędzia cyberbezpieczeństwa**.

*Accenture, raport "2020 Cyber Threatscape"

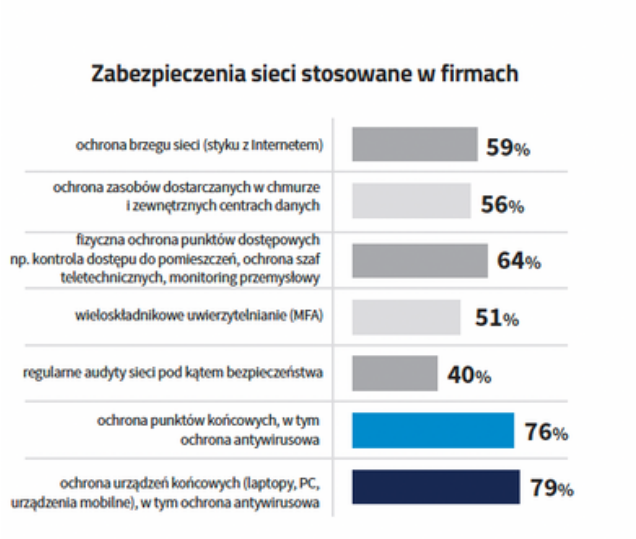


Pełen raport można pobrać po zeskanowaniu kodu QR.

Zabezpieczenia stosowane w firmach

Firmy stosują szereg komplementarnych zabezpieczeń sieci mających chronić systemy, aplikacje i dane przed zagrożeniami wewnętrznymi i zewnętrznymi. Z wyników badania można wysnuć wniosek, że poziom adaptacji różnego rodzaju zabezpieczeń jest zbliżony, niezależnie od wielkości firmy.

Zabezpieczamy się...



...ale nie weryfikujemy poprawności naszych zabezpieczeń.



Zmiany w bezpieczeństwie wymuszone przez COVID

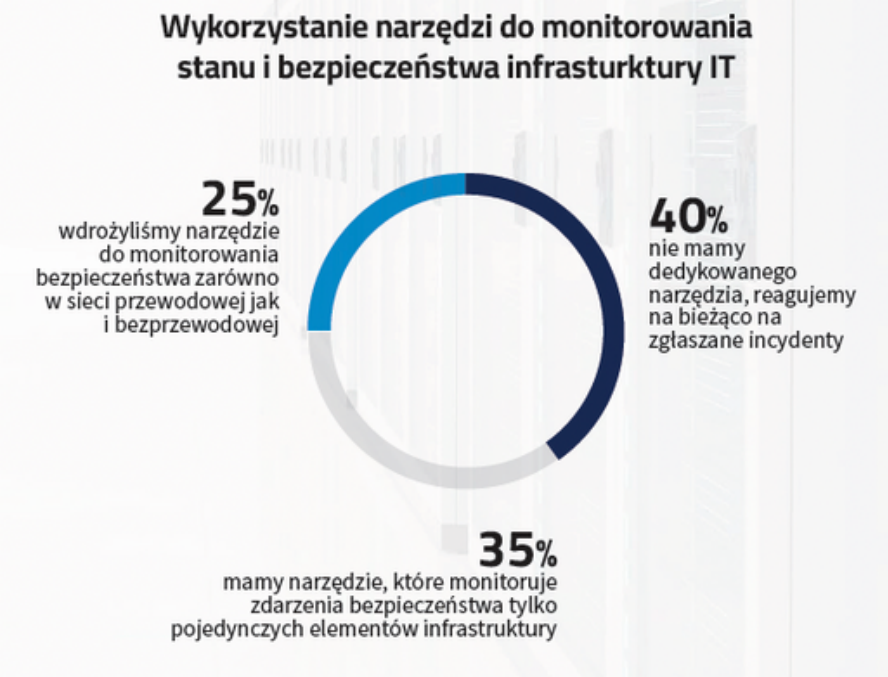


*Grandmetric & Computerworld, badanie "Infrastruktura IT przedsiębiorstw produkcyjnych w dobie pandemii COVID-19, 2021

Jak sprawdzamy poziom zabezpieczeń?

60% firm posiada narzędzia do monitorowania stanu i bezpieczeństwa infrastruktury IT.

25% wdrożyło je do śledzenia stanu bezpieczeństwa sieci przewodowej i bezprzewodowej, a 35% dysponuje narzędziem, które monitoruje zdarzenia bezpieczeństwa tylko pojedynczych elementów infrastruktury.



Problem 1.

Rozproszenie systemów monitoringu stanowi poważne wyzwanie dla działów IT, które z różnych odbieraj coraz więcej alertów o naruszeniu bezpieczeństwa.

Problem 2.

Aż 40% ankietowanych nie wdrożyło żadnych dedykowanych narzędzi w tym obszarze i tylko **na bieżąco reaguje na zgłaszane incydenty**. Takie podejście powoduje z czasem utratę kontroli i bierne reagowanie na pojawiające si problemy.

Problem 3.

Wyniki badania potwierdzają obiegową opinię, że w obszarze bezpieczeństwa wdraża się rozwiązania techniczne, a nie organizacyjne. 56% ankietowanych z rozbrajającą szczerością przyznało, że **nie szkoli pracowników w zakresie cyberbezpieczeństwa**.

Rekomendacje

Kupujemy sprzęt IT wysokiej jakości, ale nierzadko zapominamy o tym, że sam **sprzęt nie gwarantuje bezpieczeństwa ani poprawnego działania**.

To, co najczęściej obserwujemy podczas audytów, nawet w dużych i znanych firmach, to brak zarządzania politykami dostępu, źle skonfigurowane urządzenia brzegowe takie jak UTM czy Firewall, ale też podatność na proste zabiegi social engineering.

W dobie zapowiadanych po długiej przerwie powrotów do biur, polskie firmy powinny zwrócić szczególną uwagę na budowanie świadomości personelu. Bez solidnej edukacji nawet najlepszy sprzęt nie ochroni firmy przed utratą danych.

1. Dbaj o **regularne aktualizacje** systemów i aplikacji.

2. Przeprowadzaj **regularne audyty** infrastruktury i bezpieczeństwa.

3. **Regularnie szkol** pracowników w zakresie potencjalnych ataków.

4. Wymuś korzystanie z mocnych haseł i **regularnie je zmieniaj**.

Więcej o cyberbezpieczeństwie

Po więcej informacji o bezpieczeństwie cyfrowym **zapraszamy do rozmowy z naszymi ekspertami** w Strefie Partnerskiej oraz do naszego podcastu Próba Połączenia, w którym poruszaliśmy zagadnienia cybersecurity.







Kontakt

Grandmetric sp. z o.o.
ul. Metalowa 5
60-118 Poznań
www.grandmetric.com/pl
info@grandmetric.com

GRANDMETRIC
STAY CONNECTED.