Czy jesteś przygotowany na wszystko?

Wydarzenia roku 2020 pokazały, że obecnie odporność na cyberataki jest ważniejsza niż kiedykolwiek wcześniej. Analizy NTT i Cisco.

Wnioski oparte na danych

Kluczowe wnioski z dorocznego raportu bezpieczeństwa przygotowanego przez NTT i Cisco

Co to jest cyberodporność?

Cyberodporność to zdolność do ciągłego utrzymywania normalnego funkcjonowania firmy dzięki skutecznej ochronie przed zagrożeniami i coraz bardziej wyrafinowanymi atakami. Pojęcie to obejmuje elastyczne podejście do zapobiegania atakom, szybsze wykrywanie i likwidowanie naruszeń bezpieczeństwa oraz minimalizowanie ich skutków.

Natężenie ataków wzrosło w latach 2018-2019 ze względu na popularność takich narzędzi jak web shell, zestawy exploitów i ukierunkowany ransomware, a dodatkowo siła ich rażenia jest wzmacniana poprzez korzystanie ze sztucznej inteligencji (AI), uczenia maszynowego (ML) i automatyzacji.

Zmiana krajobrazu zagrożeń

Ataki przyjmują zróżnicowaną formę, co utrudnia ich zwalczanie.
Same firmy niejako ułatwiają przestępcom działanie – nie korzystają z dobrych praktyk cyberbezpieczeństwa.
Potwierdzają to wyniki naszych najnowszych badań:

- **Cyberprzestępcy wykorzystują AI i ML** oraz inwestują w automatyzację ataków
- **21% wykrytego złośliwego oprogramowania** miało formę skanera podatności na ataki
- Zdalne wykonanie kodu (RCE) jest najpopularniejszą techniką, stanowiącą **15% wszystkich ataków**
- Urządzenia IoT nadal są **narażone na ataki**
- **Zidentyfikowano 258 nowych luk** we frameworkach i oprogramowaniu Apache
- **Prawie 55% wszystkich ataków** stanowiły ataki na aplikacje (33%) i aplikacje internetowe (22%)

Rok 2019 był rokiem wprowadzania w życie zasad GRC (zarządzanie bezpieczeństwem, ryzykiem i zgodnością), ale jest to obszar coraz bardziej złożony i trudny do opanowania.

Źródło: NTT Ltd. Global Threat Intelligence Report 2020

Stare podatności nadal stanowią cel ataków

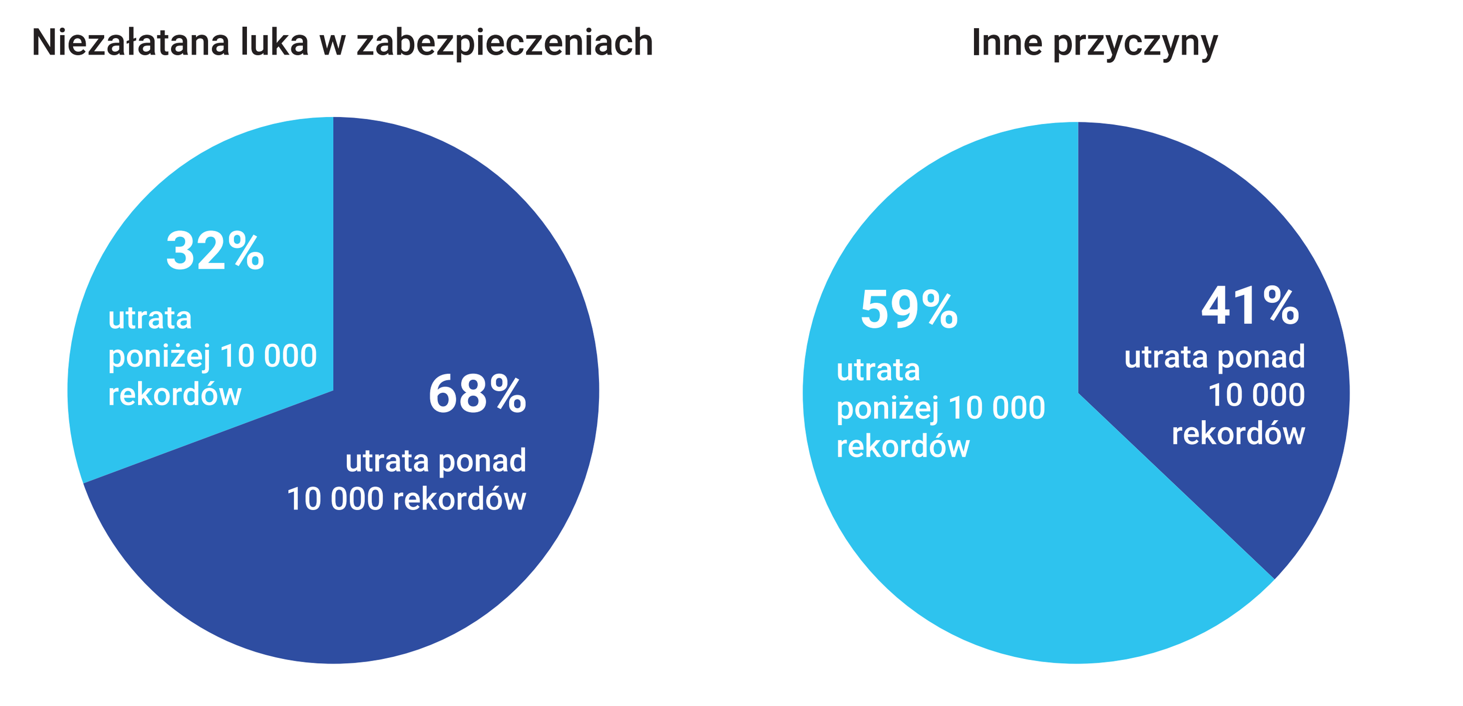
Nadal obserwujemy ataki na znane od dawna luki w zabezpieczeniach, pomimo dostępności łat, ponieważ organizacje nadal są otwarte na te podatności, nie stosując najlepszych praktyk.[1]

W 2019 roku 46% organizacji

zanotowało incydenty spowodowane niezałataną luką w zabezpieczeniach.

(rok wcześniej było to tylko 30%[2])

Firmy, w których doszło do poważnego naruszenia bezpieczeństwa z powodu niezałatanej luki w zabezpieczeniach, doświadczyły wyższego poziomu utraty danych.



Źródło: Cisco 2020 CISO Benchmark Survey

Do wzrostu zagrożeń związanych z bezpieczeństwem przyczyniają się masowe zmiany, rozproszone środowiska i obciążenia pracą oraz konieczność pracy zdalnej i mobilnej.

Z każdym dniem jest coraz więcej urządzeń IoT
Do 2025 roku 41,6 mld urządzeń będzie podłączonych do do sieci[3]

Elementy pracy i aplikacje są przenoszone do chmury
Do 2025 roku 80% przetwarzania danych w firmach zostanie przeniesionych do chmury[4]

Użytkownicy pracują w dowolnym miejscu na różnych urządzeniach
Do 2025 roku prawie 80% całego ruchu w sieci będzie pochodzić z urządzeń bezprzewodowych i mobilnych[5]

Bezpośredni dostęp do internetu w firmach o rozproszonej strukturze
Z analiz wynika, że średnie tempo wzrostu rynku SD-WAN w latach 2018 – 2023 wyniesie 74%, dzięki wzmożonemu popytowi na usługi DIA (Direct Internet Access)[6]

Zaobserwowaliśmy gwałtowny wzrost liczby ataków na urządzenia IoT, szczególnie w obu Amerykach. Jest to rynek, gdzie Internet Rzeczy jest rozpowszechniony, ale nieposiadający rozwiniętych i skutecznych zabezpieczeń w tym sektorze.

Złożoność systemów IT prowadzi do rozproszenia i osłabienia ich mechanizmów obronnych

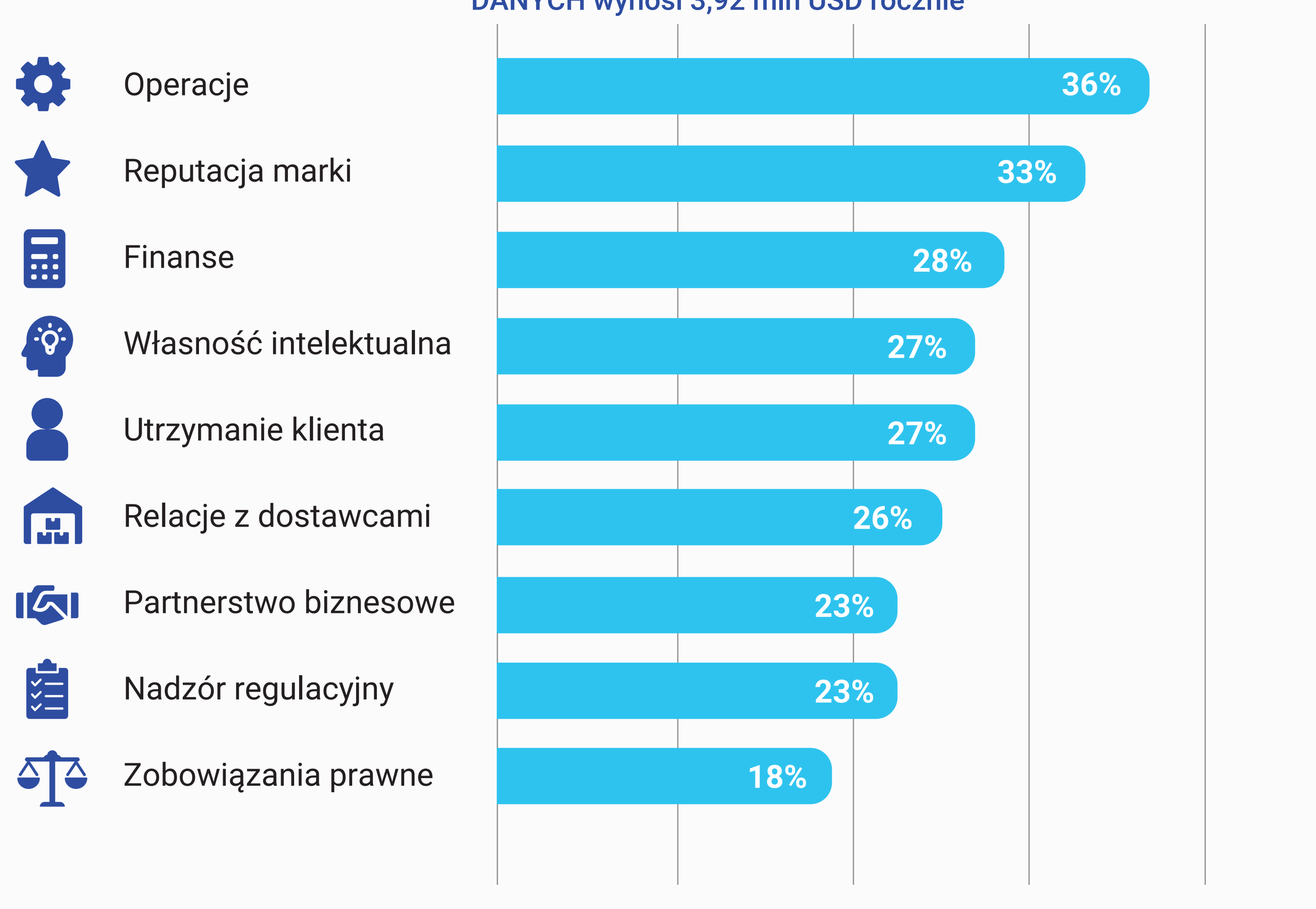
Z powodu rosnącej złożoności systemów IT i różnorodności zagrożeń, organizacje zaczęły szukać wsparcia u wielu dostawców w celu wzmocnienia bezpieczeństwa. Doprowadziło to do zwiększenia liczebności zespołów zajmujących się bezpieczeństwem oraz nadmiaru alertów i sygnałów do przeanalizowania.

- **42%** przedsiębiorstw odczuwa przeciążenie związane z analizą wszystkich alertów, więc zrezygnowało z proaktywnej obrony
- **96%** osób pracujących na wielu systemach równolegle uważa, że zarządzanie środowiskiem wielu dostawców jest dużym wyzwaniem
- **93%** osób zajmujących się pracą na wielu systemach otrzymuje ponad 5 000 alertów każdego dnia

Źródło: Cisco 2020 CISO Benchmark Survey

Obszary, w których skutki utraty danych są wyjątkowo bolesne

Skutki finansowe: średni całkowity KOSZT NARUSZEŃ BEZPIECZEŃSTWA DANYCH wynosi 3,92 mln USD rocznie[7]

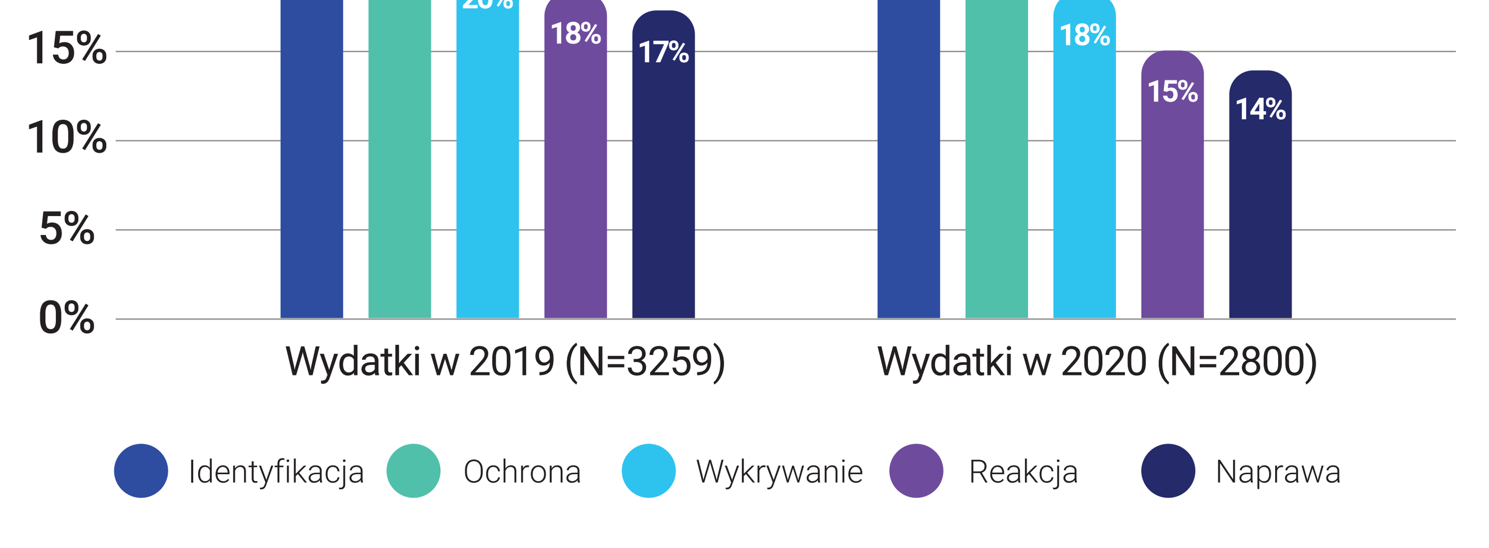


Źródło: Cisco 2020 CISO Benchmark Survey

Zagrożenie dla marki firmy wzrasta. Uderzenie w reputację marki w wyniku poważnych naruszeń bezpieczeństwa wzrosło z 26% do 33% w ciągu ostatnich trzech lat. Kluczowe jest uwzględnienie strategii komunikacji kryzysowej w planie reagowania na incydenty. W przypadku naruszenia bezpieczeństwa najlepiej działać transparentnie: **61% organizacji odnotowało wzrost wiarygodności po dobrowolnym ujawnieniu poważnego naruszenia.**

Bądź proaktywny i przewidujący

Zaobserwowane ostatnio zmiany w wydatkach wskazują, że wraz ze wzrostem nakładów na lepszą identyfikację zagrożeń, wzrasta chęć bycia bardziej proaktywnym i przewidującym. Ogólny trend pokazuje, że **organizacje wydają więcej na zapobieganie, niż na reaktywność.**



Źródło: Cisco 2020 CISO Benchmark Survey

NTT i Cisco pomagają identyfikować, ograniczać skutki i reagować na zagrożenia bezpieczeństwa

Złożoność systemów IT i przeciążenie ciągłymi alertami związanymi z bezpieczeństwem nadwyrężają zasoby ludzkie zespołów bezpieczeństwa firm. W takiej sytuacji pomocne może być zwrócenie się do zaufanego partnera. **34% firm korzysta z usług zewnętrznych w zakresie reagowania na zagrożenia bezpieczeństwami, a 36% korzysta z usług firm trzecich w celu analizy zagrożonych systemów.**

NTT i Cisco dostarczają najlepsze w swojej klasie technologie i usługi, które podwyższają standardy bezpieczeństwa organizacji, minimalizują zagrożenia i przyspieszają reakcję na incydenty.

Razem pomożemy Twojej organizacji

Redukować ryzyko
Dbać o zapewnienie bezpieczeństwa we wszystkich inicjatywach związanych z transformacją cyfrową

Zapewniać zgodność z przepisami
Dostosowywać działania do rosnącej liczby przepisów poprzez zwiększoną przejrzystość, automatyzację i sprawniejsze raportowanie

Przewidywać zagrożenia i proaktywnie im zapobiegać
Identyfikując możliwe zagrożenia i zabezpieczając się przed atakami - zanim one nastąpią

Nieustannie wprowadzać innowacje
Zadbać o to, żeby podejście do cyberbezpieczeństwa i plan działań w zakresie technologii odpowiadały obecnym i przyszłym potrzebom

Szybko likwidować skutki
Natychmiast identyfikować, reagować i ograniczać siłę rażenia ataku, aby jak najszybciej powrócić do normalnej działalności

Dlaczego NTT i Cisco?

Od ponad 28 lat pracujemy razem, aby wspomagać organizacje na całym świecie w wykorzystywaniu technologii do wprowadzania innowacji.

Służymy naszym globalnym doświadczeniem klientom
w 47 krajach

Łącznie pracuje dla nas ponad 6 000
specjalistów ds. cyberbezpieczeństwa na całym świecie

Posiadamy wspólne centra innowacji
na całym świecie w celu szybszego zaspokajania potrzeb klientów

Obsługujemy ponad 5000
wspólnych klientów na całym świecie

Codziennie analizujemy 9,5 terabajtów danych,
żeby pomóc Ci znaleźć igłę w stogu siana

Jesteśmy zaangażowani społecznie
na rzecz ludzi, społeczeństwa i naszej planety

Jak możemy Ci pomóc zajść dalej?

Dowiedz się więcej o rozwiązaniach w zakresie bezpieczeństwa oferowanych przez NTT i Cisco.

Zapisz się, aby otrzymywać Cisco Talos Newsletter

Zasubskrybuj Miesięczny Raport Zagrożeń i Komunikaty o Zagrożeniach od firmy NTT.

Źródła:

1. NTT Ltd. Global Threat Intelligence Report 2020
2. Cisco 2020 CISO Benchmark Survey
4. Oracle's Top 10 Cloud Predictions 2019
5. https://cybersecurityventures.com/mobile-security-report-2017/
6. Apps Run The World, "Top 10 SD-WAN Software Vendors, Market Size and Market Forecast 2018-2023", Dec 2019
7. Ponemon, Cost of a Data Breach Study, 2019