Acronis

RAPORT

Service Providerzy mogą zamienić rosnące zagrożenie atakami ransomware w źródło przychodów

Jak rozwinąć firmę dzięki usługom w zakresie ochrony przed cyberzagrożeniami

Według raportu Juniper Research cyberprzestępczość to dynamicznie rozwijający się biznes. Wyrządza firmom szkody szacowane na 3 biliony dolarów rocznie, a do 2024 r. kwota ta ma wzrosnąć do 5 bilionów dolarów.[1] Cyberataki są kosztownym koszmarem wielu przedsiębiorstw prowadzącym do przestojów skutkujących utratą zysków, do utraty przychodów, uszkodzenia wizerunku marki, spadku cen akcji i kar finansowych.

Raport na temat gotowości do zapewnienia bezpieczeństwa cybernetycznego Acronis, w którym zbadano 3400 menedżerów IT i pracowników zdalnych z całego świata w celu oceny ich gotowości do zapewnienia bezpieczeństwa cybernetycznego przed pandemią COVID-19 i po pandemii, wykazał, że 31% firm z całego świata jest atakowanych przynajmniej raz dziennie. Ponadto 50% respondentów przyznało, że w ciągu ostatnich trzech miesięcy doświadczyło ataku cybernetycznego przynajmniej raz w tygodniu.[2] W międzyczasie wielu badaczy wywnioskowało, że koszty przestoju mogą wynosić od 10 000 USD za godzinę[3] do aż 260 000 USD za godzinę[4].

Spośród wszystkich rodzajów złośliwego oprogramowania ransomware jest obecnie najbardziej wszechobecnym cyberzagrożeniem. Między trzecim kwartałem 2019 r. a trzecim kwartałem 2020 r. ataki ransomware wzrosły o 139%[5]. Do ataków ransomware dochodziło w tym okresie we wszystkich branżach. Na przykład, w trzecim kwartale 2020 r. liczba skutecznych ataków ransomware na sektor edukacji wzrosła o 388%[6].

> Nic dziwnego, że kierownicy firm i menedżerowie IT niepokoją się, że atak mógłby w końcu doprowadzić do likwidacji ich firmy.

Ransomware skutecznie narusza bezpieczeństwo ofiar (często po prostu zachęca nieuważnego pracownika do kliknięcia na e-mail phishingowy) i powoduje nagłe zamknięcia systemu, co zakłóca działanie firmy i szybko przedostaje się do opinii publicznej. Poza tym płatności za pomocą kryptowalut utrudniają działania organów ścigania. To prostsze i bardziej dochodowe przestępstwo niż przełamywanie zabezpieczeń w celu kradzieży i odsprzedaży poufnych danych.

RANSOMWARE: ZAGROŻENIE I SZANSA

Jako Service Provider na pewno zdajesz sobie sprawę z tego, że ta fala cyberprzestępstw jest zarówno zagrożeniem, jak i szansą.

Zagrożenie częściowo wynika z faktu, że dostawcy technologii i Service Providerzy są wykorzystywani do dotarcia do klientów biznesowych i instytucji rządowych w złożonych atakach w łańcuchu dostaw: najsłynniejszym takim przypadkiem było naruszenie SolarWinds wykryte w grudniu 2020 r.[7] Włamując się do firm programistycznych i osadzając złośliwe oprogramowanie w popularnych aplikacjach, cyberprzestępcy mogą naruszyć bezpieczeństwo Service Providerów korzystających z tych narzędzi – a z tego miejsca także bezpieczeństwo klientów, których infrastrukturą IT zarządzają[8].

Jednak znalezienie się na celowniku hakerów stosujących ransomware to tylko jedno oblicze zagrożenia – niemożność powstrzymania ataków ransomware na klientów szkodzi konkurencyjności i zdolności rozwoju Service Providerów. Dla Service Providerów to wyzwanie staje się coraz większe i coraz bardziej skomplikowane. Statystyki pokazują, że:

71%

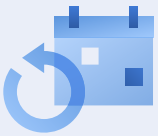
ataków ransomware jest wymierzonych w **małe i średnie przedsiębiorstwa (MŚP)**[8]

3 z 5

Service Providerów **musiało zmierzyć się** w poprzednim roku z atakiem ransomware na swoich klientów spośród MŚP[9]

24%

MŚP **już zmieniło** swoich Service Providerów w następstwie cyberataku[10]



52%

MŚP twierdzi, że brakuje im wewnętrznych umiejętności potrzebnych do właściwego radzenia sobie z kwestiami bezpieczeństwa[11]

TYLKO 31%

Service Providerów jest **w pełni przekonana** co do swojej zdolności ochrony klientów przed przyszłymi atakami ransomware[12]

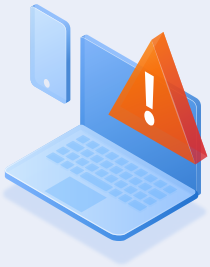
74%

MŚP współpracujących z Service Providerami powiedziało, że podjęłoby **działania prawne przeciw swojemu dostawcy usług**, jeśli stałyby się ofiarami cyberataku[13]

Każde wyzwanie biznesowe stanowi także okazję. Musisz chronić się przed atakami ransomware i zatrzymać ich rozpowszechnianie. Istnieje również możliwość utworzenia nowych, wysoce dochodowych i zróżnicowanych ofert dla Twoich klientów. Możesz zaoferować im usługi ochrony przed cyberzagrożeniami, które obronią ich przed oprogramowaniem ransomware i innymi zagrożeniami prowadzącymi do utraty danych. Zwróć uwagę na następujące dane:

NAJWAŻNIEJSZE CZYNNIKI WZROSTU BUDŻETU IT W 2021 R.[14]

1. Potrzeba uaktualnienia przestarzałej infrastruktury IT



2. Większy priorytet projektów IT

3. Większe obawy dotyczące bezpieczeństwa

89%

Odsetek MŚP, które **wzięłyby pod uwagę zatrudnienie nowego Service Providera**, jeśli zaoferowano by im odpowiednie rozwiązanie do ochrony przed cyberzagrożeniami[15]

25%

Wzrost rocznych kosztów, które **gotowe są pokryć** firmy już korzystające z usług Service Providera, aby uzyskać „odpowiednie rozwiązanie z zakresu cyberbezpieczeństwa" od nowego dostawcy[16]

89%

Odsetek MŚP niekorzystających z usług Service Providera, które **wzięłyby pod uwagę zatrudnienie takiego dostawcy**, jeśli zaoferowano by im „odpowiednie rozwiązanie z zakresu cyberbezpieczeństwa"[17]

Propozycja wartości, którą możesz przedstawić swoim klientom z małych i średnich przedsiębiorstw, jest prosta i przekonująca: „Dzięki nam zagrożenie atakami ransomware i innymi rodzajami złośliwego oprogramowania nie będzie już Twoim zmartwieniem. Ochronimy Cię również przed wieloma innymi przypadkami utraty danych."

Wyzwanie polega na tym, aby ta oferta była atrakcyjna i opłacalna, co oznacza, że musi być prosta, łatwa do zarządzania, kompatybilna z istniejącą infrastrukturą oraz obarczona wysoką marżą.

TRZY POPULARNE METODY, ZA POMOCĄ KTÓRYCH SERVICE PROVIDERZY ZWALCZAJĄ RANSOMWARE ORAZ ICH OGRANICZENIA

Rozwiązania, które dostępne są dostawcom usług zarządzanych w celu zwalczania ransomware zwykle należą do jednej z trzech kategorii: backup, backup z ograniczoną ochroną przed ransomware oraz backup połączony z zewnętrznym programem chroniącym przed złośliwym oprogramowaniem na punktach końcowych.

Każde z tych rozwiązań ma pewne ograniczenia:

1. Działanie samego **backupu** polega na przywracaniu zaatakowanych systemów do punktu w czasie poprzedzającego atak. Ale stosowanie samego backupu ma kilka wad. Przywracanie dziesiątek lub setek systemów z kopii zapasowej (zwłaszcza z wolniejszych nośników, takich jak taśma lub chmura) może być czasochłonne, uciążliwe dla biznesu i niezwykle kosztowne.[18] Poza tym punkt odzyskiwania może być tak odległy w czasie, że wiele cennych danych utworzonych pomiędzy backupem a atakiem zostanie utraconych.

2. Backup z ograniczoną ochroną przed ransomware może pokonać niektóre ataki, ograniczając potrzebę polegania na samym backupie w celu odzyskania danych. Jednak wykrywanie ataku zwykle polega na niedokładnych miarach statystycznych w celu porównania tempa zmian plików z progiem bazowym. Nagły wzrost szybkości zmian plików wskazuje na możliwy atak. Niestety, takie podejście jest reaktywne i podatne zarówno na błędy wykrywania, jak i fałszywe alarmy, co z kolei wiąże się ze znacznymi kosztami. Podobnie jak w przypadku samego ataku to rozwiązanie nie będzie pomocne, jeśli atak zdoła zlokalizować i naruszyć backupy (a potrafi to wiele wersji ransomware), całkowicie udaremniając proces odzyskiwania danych.

3. Backup połączony z zewnętrznym programem chroniącym przed złośliwym oprogramowaniem na punktach końcowych stara się stosować bardziej wyrafinowane metody ochrony punktów końcowych przed oprogramowaniem ransomware. Jednak brak integracji pomiędzy tymi dwoma komponentami i ich agentami często prowadzi do problemów z wydajnością systemu, konfliktów procesów, które mogą zakłócić tworzenie kopii zapasowych oraz do wyzwań dla MSP związanych z wdrażaniem i zarządzaniem.

BARDZIEJ ZAAWANSOWANA I SKUTECZNIEJSZA OPCJA DLA SERVICE PROVIDERÓW

Czwarta alternatywa oferuje Service Providerom prostsze, skuteczniejsze i wydajniejsze rozwiązanie: technologia Acronis Cyber Protect Cloud z Acronis Active Protection. To rozwiązanie stosowane przez ponad 10 000 Service Providerów umożliwia świadczenie usług z zakresu ochrony przed cyberzagrożeniami, które łączą backup jako usługę ze zintegrowanymi funkcjami cyberbezpieczeństwa opartymi na AI (w tym program antywirusowy, program chroniącym przed złośliwym oprogramowaniem i program chroniący przed cryptojackingiem) oraz z automatycznymi funkcjami naprawy:

- Acronis Active Protection stosuje sztuczną inteligencję (AI) i uczenie maszynowe (ML) do wykrywania i unieszkodliwiania cyberataków. Ciągłe szkolenie zaawansowanego silnika wykrywania behawioralnego w infrastrukturze Acronis Cloud AI zapewnia najniższy w branży wskaźnik fałszywych alarmów w wykrywaniu złośliwego oprogramowania, w tym ataków typu „zero day" (tj. wcześniej nieznanych).
- Zintegrowane mechanizmy samoobrony uniemożliwiają atakom ransomware narażenie procesów tworzenia kopii zapasowych, agentów i archiwów Acronis.
- Automatyczna naprawa korzysta z lokalnej cache, aby szybko przywrócić wszelkie pliki uszkodzone przed wykryciem ataku, zapewniając natychmiastowe wznowienie działalności biznesowej bez konieczności pełnego przywracania danych z kopii zapasowej.
- Oceny podatności na zagrożenia i zautomatyzowane zarządzanie poprawkami zamykają luki w zabezpieczeniach, które wpuszczają oprogramowanie ransomware do systemu, a filtrowanie adresów URL blokuje strony internetowe rozpowszechniające złośliwe oprogramowanie.
- Ten sam zaawansowany silnik wykrywania behawioralnego identyfikuje i przerywa ataki typu cryptojacking, które potajemnie zużywają zasoby systemowe w celu nielegalnego wydobywania kryptowalut – co jest kosztownym obciążeniem dla wydajności systemu, zasobów zasilania i chłodzenia. To popularne zagrożenie złośliwym oprogramowaniem ożywiło się w 2020 r., gdy wzrosły wartości kryptowalut[19].

Krótko mówiąc, wyjątkowa integracja backupu, cyberbezpieczeństwa i zarządzania punktami końcowymi oferowana przez Acronis Cyber Protect Cloud umożliwia Ci natychmiastowe ograniczenie narażania Twoich klientów na ransomware. Aby zyskać pełną ochronę przed cyberzagrożeniami, wystarczy zainstalować jednego agenta, co pomoże także uniknąć konfliktów między procesami i problemów z wydajnością.

„Rozwiązanie Acronis zapewnia doskonałą wydajność, jest łatwe w użyciu i ma obszerny zestaw funkcji. Poza tym jest to jedyne rozwiązanie w teście, które zapewnia specjalną ochronę przed atakami ransomware. Dzięki temu firma Acronis otrzymała pierwszy w historii certyfikat AV-TEST w zakresie backupu i ochrony danych."

David Walkiewicz
dyrektor ds. badań testowych,
av-test.org

ŚWIADCZENIE USŁUG Z ZAKRESU OCHRONY PRZED CYBERZAGROŻENIAMI ZA POMOCĄ ROZWIĄZAŃ ACRONIS

Jednak Service Providerzy mogą zyskać znacznie więcej niż tylko zaawansowane możliwości ochrony przed ransomware. Acronis Cyber Protect Cloud należy do Acronis Cyber Cloud, wielousługowej platformy ochrony przed cyberzagrożeniami stworzonej z myślą o Service Providerach. To Twój **szwajcarski scyzoryk do świadczenia usług z zakresu ochrony przed cyberzagrożeniami, który oferuje:**

1. Zintegrowany zestaw rozwiązań obejmujący **najlepszy w swojej klasie backup, odzyskiwanie po awarii, cyberbezpieczeństwo (w tym program antywirusowy, program chroniący przed złośliwym oprogramowaniem, przed ransomware i cryptojackingiem), synchronizację i udostępnianie plików, poświadczanie plików, pamięć masową zdefiniowaną programowo i zarządzanie punktami końcowymi.**
2. **Platformę** do ujednoliconego świadczenia usług, zarządzania kontami, monitorowania, integracji, sprzedawania produktów pod marką dystrybutora i nie tylko.

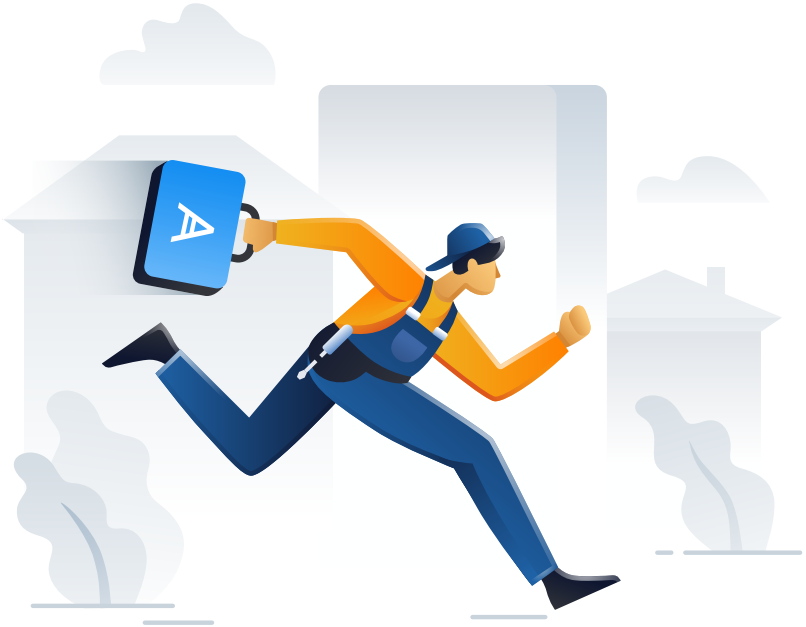
Oferując Acronis Cyber Protect Cloud, Service Providerzy mogą świadczyć zyskowne usługi z zakresu ochrony przed cyberzagrożeniami o niskim wskaźniku migracji klientów, które pozwolą klientom bez obaw prowadzić działalność w świecie, który jest coraz bardziej zagrożony cyberprzestępczością. Poza tym Service Providerzy mogą działać z najwyższą wydajnością – od wstępnego wdrożenia systemu po ujednolicone świadczenie usług i zarządzanie klientami. Platforma Acronis Cyber Cloud obejmuje:

- wielodostępowość w celu obsługi nieograniczonej liczby klientów,
- wielousługowy portal zarządzania,
- funkcje sprzedaży pod marką dystrybutora do łatwego brandingu,
- limity użytkowania usług i raportowanie,
- integrację z najpopularniejszymi narzędziami PSA i RMM,
- niestandardowe integracje dodatkowych usług za pośrednictwem otwartego API.

Dowiedz się, w jaki sposób Acronis umożliwi Ci świadczenie usług ochrony przed cyberzagrożeniami w łatwy, skuteczny i bezpieczny sposób:

Skontaktuj się z działem sprzedaży Acronis, aby umówić się na demonstrację produktu na żywo dostosowaną do Twoich przypadków zastosowania. **KONTAKT Z DZIAŁEM SPRZEDAŻY**

Rozpocznij bezpłatną 30-dniową wersję próbną już dziś. **WYPRÓBUJ TERAZ**



Źródła

[1] https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security

[2] https://www.acronis.com/en-us/resource-center/resource/532

[3] https://www.cloudradar.io/cost-of-downtime

[4] https://www.stratus.com/assets/aberdeen-maintaining-virtual-systems-uptime.pdf

[5] https://securityboulevard.com/2021/02/ransomware-trends-you-need-to-know-in-2021/

[6] https://securityboulevard.com/2020/11/successful-ransomware-attacks-on-education-sector-grew-388-in-q3-2020/

[7] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[8] https://www.acronis.com/en-us/blog/posts/defending-against-supply-chain-attacks-solarwinds-breach

[9] https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

[10] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[11] https://www.connectwise.com/globalassets/media/assets/ebook/the-state-of-smb-cybersecurity-2020.pdf

[12] https://www.channele2e.com/influencers/msp-survey-shows-ongoing-ransomware-malware-challenges/

[13] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[14] https://swzd.com/resources/state-of-it/

[15] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[16] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[17] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[18] https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

[19] https://www.darkreading.com/vulnerabilities---threats/cryptojacking-the-unseen-threat/a/d-id/1338903