Odzyskiwanie danych po ataku ransomware w 2022 r.

https://vee.am/RW22

Tomasz Turek
Veeam

ABC odzyskiwania po awarii

Pewność odzyskania obciążenia

Czy masz niezawodne kopie danych na potrzeby odzyskiwania?

Kopie zapasowe o zweryfikowanej odzyskiwalności

Odzyskiwanie na dużą skalę

Jak możesz skrócić rzeczywisty czas odzyskiwania?

Zorkiestrowane procesy robocze

Odzyskiwanie do alternatywnej infrastruktury

Czy jesteś w stanie zacząć od zera?

W chmurze hybrydowej lub między platformami

Awaria sprzętu

Uszkodzenie

Pożar

Powódź

Burza

VEEAM

ABC odzyskiwania po awarii

Pewność odzyskania obciążenia

Czy masz niezawodne kopie danych na potrzeby odzyskiwania?

Kopie zapasowe o zweryfikowanej odzyskiwalności

Odzyskiwanie na dużą skalę

Jak możesz skrócić rzeczywisty czas odzyskiwania?

Zorkiestrowane procesy robocze

Odzyskiwanie do alternatywnej infrastruktury

Czy jesteś w stanie zacząć od zera?

W chmurze hybrydowej lub między platformami

Ransomware

Awaria sprzętu

Uszkodzenie

Pożar

Powódź

Burza

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

takami ransomware
pasowe to ostatnia linia
prony

Odzyskiwanie

Natychmiastowe odzyskiwanie na dużą skalę

Bezpieczne przywracanie

Orkiestracja odzyskiwania po awarii

rogramowo, bez uzależnienia od
nego sprzętu

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

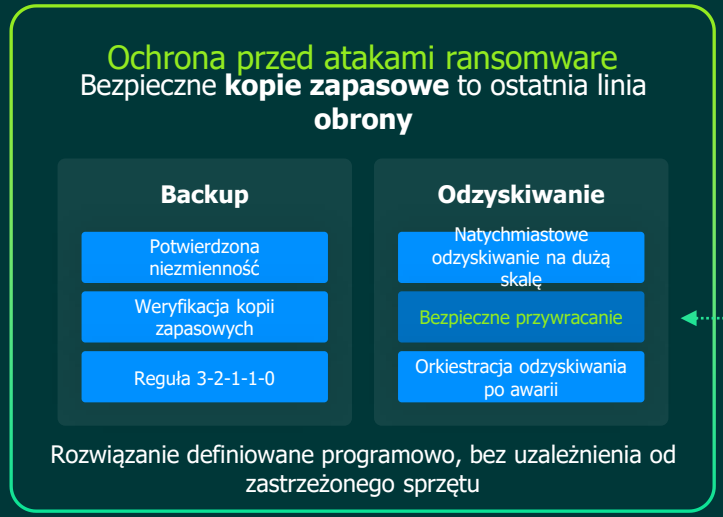
Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury



VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Częste, lepsze testowanie

84%

firm sprawdza możliwość odzyskania danych na podstawie dzienników kopii zapasowych lub możliwości odczytu nośnika — oznacza to, że tylko **16%** rutynowo przeprowadza testy polegające na przywróceniu i sprawdzeniu funkcjonalności

Czy w Państwa firmie wykonuje się automatyczną weryfikację odzyskiwania kopii zapasowych i/lub replik?

Źródło: Raport nt. trendów w ransomware w 2022 r. https://vee.am/RW22

Wybór sposobu ochrony danych

Założone wartości RPO i RTO można realizować na wiele sposobów.

Ciągła ochrona danych

Repliki

Kopie zapasowe

Pamięć masowa

Veeam DataLabs

Pomaga w dbaniu o dostępność i bezpieczeństwo, ograniczając ryzyko ataku złośliwego oprogramowania dzięki automatycznym testom i weryfikacji

Technologie

On-Demand Sandbox™

SureBackup® i SureReplica

Przywracanie etapowe

Bezpieczne przywracanie

Wykazywanie gotowości do odzyskania

Monitoruj zasoby odzyskiwania, aby mieć pewność, że będą gotowe do natychmiastowego użycia

Monitorowanie stanu zasobów odzyskiwania

- Brak problemów sprzętowych/programowych
- Zwracanie szczególnej uwagi na licencje

Sprawdzanie pojemności

- Czy masz wystarczającą pojemność na potrzeby odzyskiwania?
- Przydatnosć regularnych testów odzyskiwania po awarii

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

takami ransomware
pasowe to ostatnia linia
prony

Odzyskiwanie

Natychmiastowe odzyskiwanie na dużą skalę

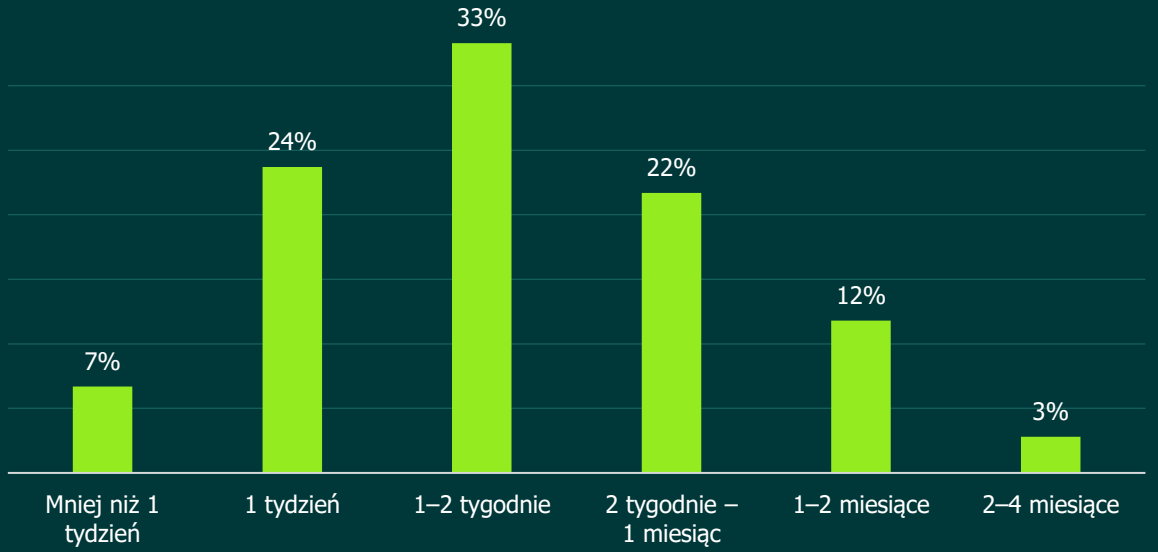
Bezpieczne przywracanie

Orkiestracja odzyskiwania po awarii

rogramowo, bez uzależnienia od
nego sprzętu

Działania naprawcze trwają nadspodziewanie długo

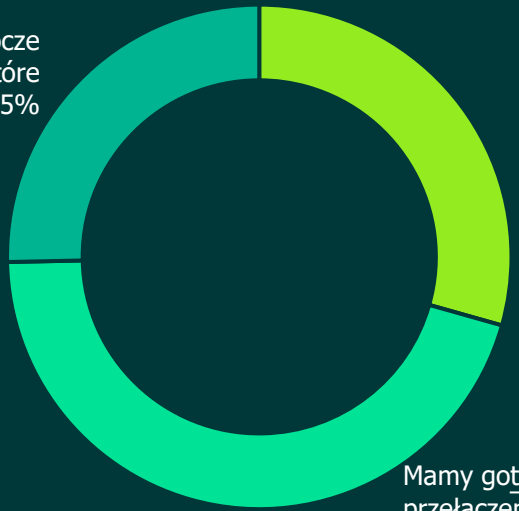
Ile trwały wszystkie działania naprawcze / operacje odzyskiwania, zanim w całej firmie można było uznać, że incydent dobiegł końca?



Źródło: Raport nt. trendów w ransomware w 2022 r.
https://vee.am/RW22

Zorkiestrowane przełączanie w tryb awaryjny

Jakiego rodzaju mechanizmy przełączania w tryb awaryjny / powrotu po awarii są stosowane w Państwa firmie z myślą o wznawianiu funkcjonowania?



Źródło: raport „Trendy w ochronie danych w 2022 r.”
https://vee.am/DPR22

Odzyskiwanie po awarii wymaga orkiestracji

Ciągła ochrona danych

Repliki

Kopie zapasowe

Pamięć masowa

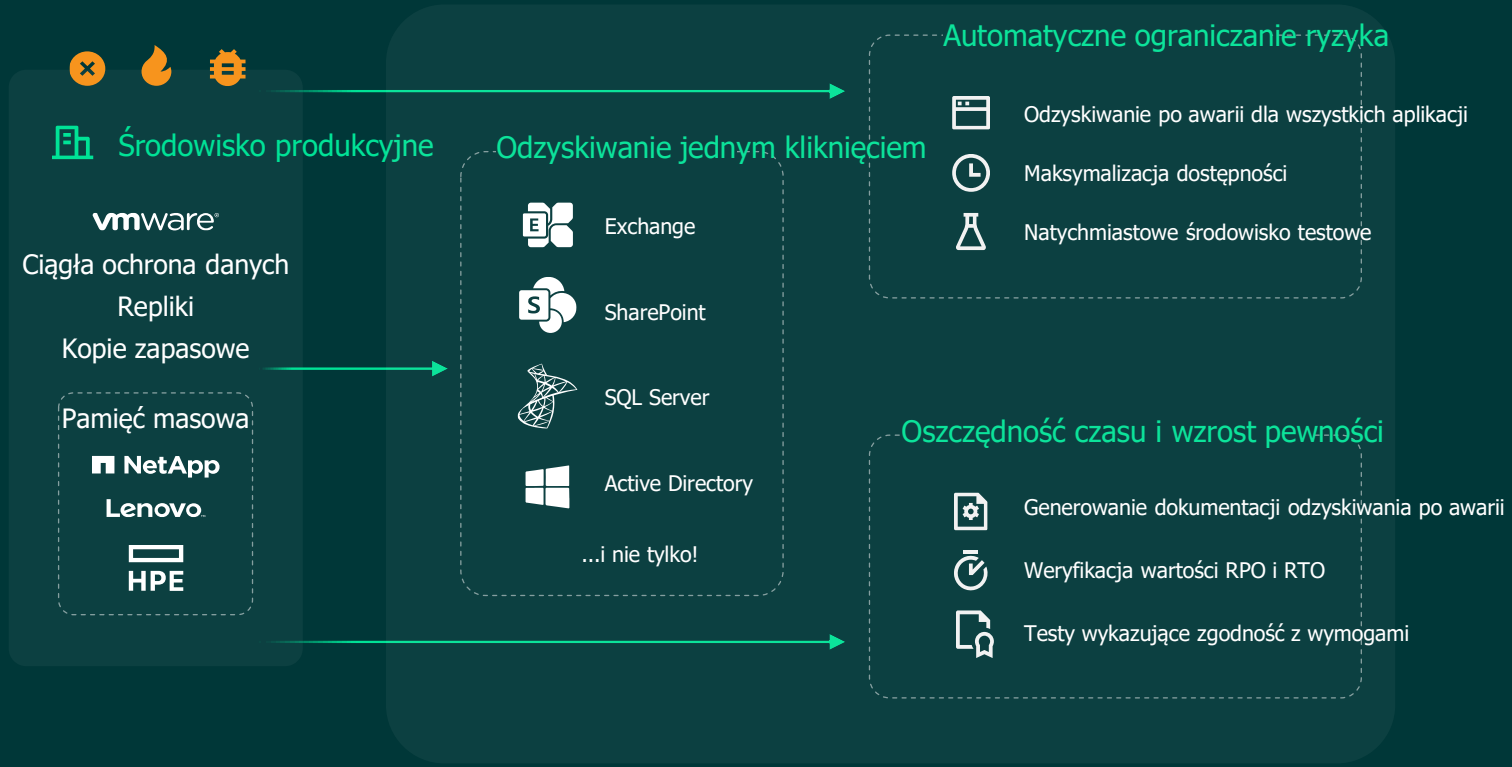
Dynamiczna dokumentacja

Automatyczne testowanie

Odzyskiwanie 1 kliknięciem

Ograniczanie ryzyka dzięki testom

Wykaż gotowość na sytuację kryzysową



Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

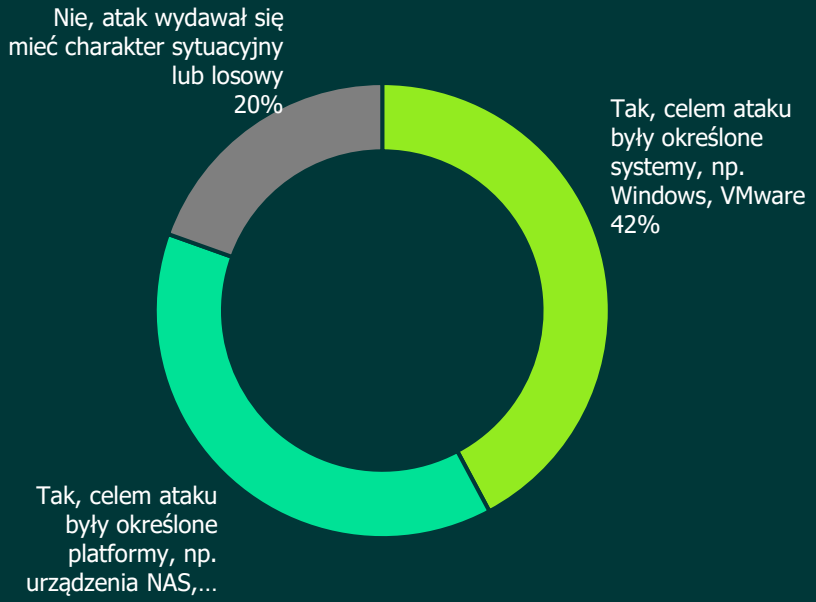
Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Ransomware: punkty wejścia i cele

Jak oprogramowanie ransomware wniknęło do środowiska IT Państwa firmy? (n=1000)

Czy atak ransomware wydawał się skoncentrowany na określonych aplikacjach lub platformach?

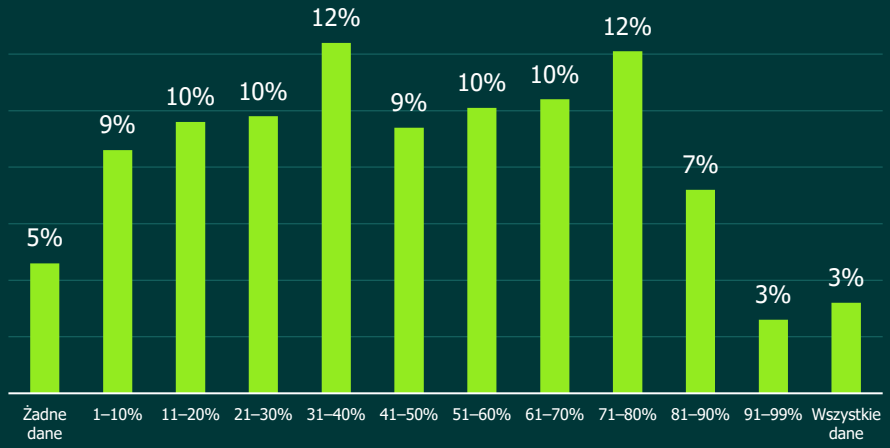


VEEAM

Ransomware: wszechobecność

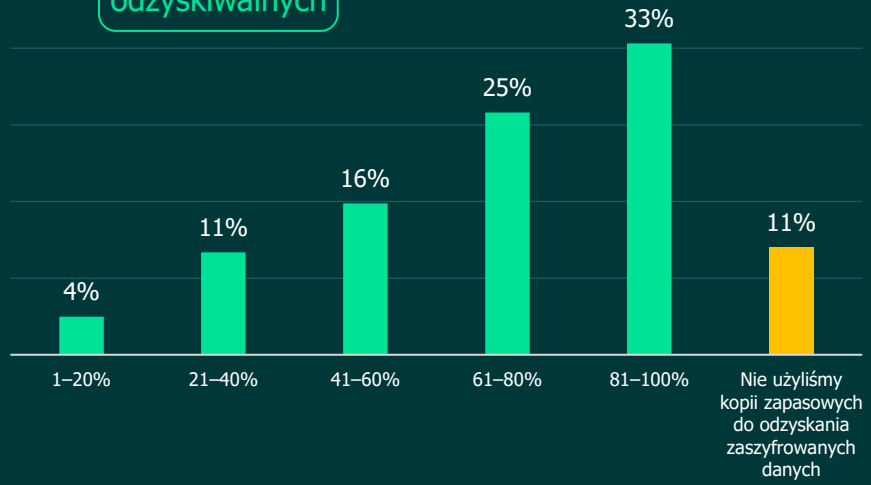
Jaki odsetek danych produkcyjnych firmy został według Państwa zaszyfrowany na skutek ataku ransomware? (n=1000)

47% zaszyfrowanych



Jaki odsetek danych udało się Państwu odzyskać po ataku przy użyciu kopii zapasowych?

69% odzyskiwalnych



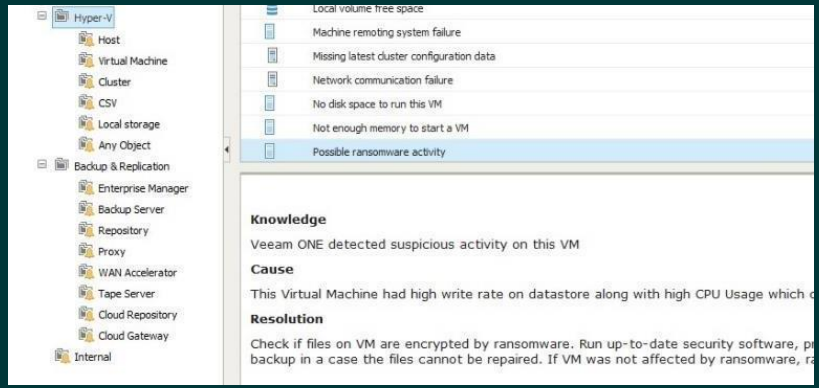
Źródło: Raport nt. trendów w ransomware w 2022 r.
https://vee.am/RW22

VEEAM

Wykrywanie nietypowej aktywności

Gotowe raporty i alarmy

- Nietypowe wykorzystanie procesora/pamięci/ sieci/we-wy itp.
- Nietypowy rozmiar przyrostowych kopii zapasowych
- Możliwość dostosowywania gotowych alarmów
- Rozwiązanie Veeam nie przekazuje nikomu danych ani zmierzonych wartości



Wartości parametrów pozyskane na odcinku sprzęt–aplikacja można wykorzystać w niestandardowych alarmach

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

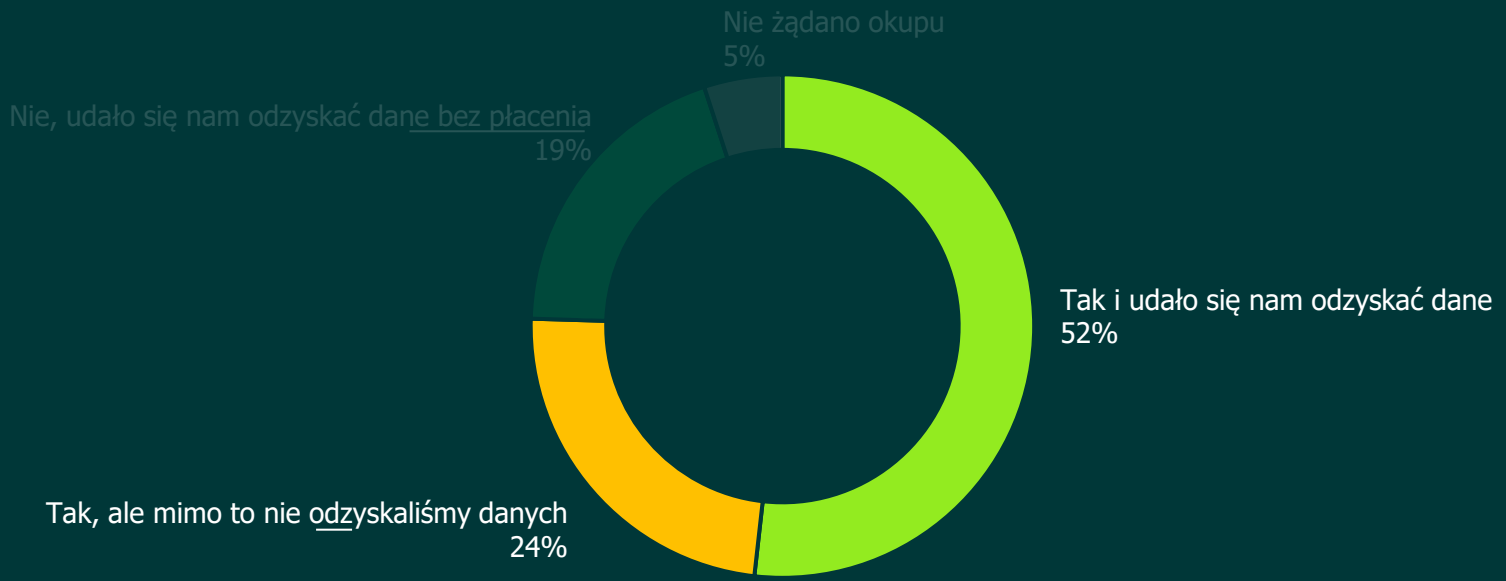
- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia zastrzeżonego sprzętu

VEEAM

Okup ≠ działanie naprawcze

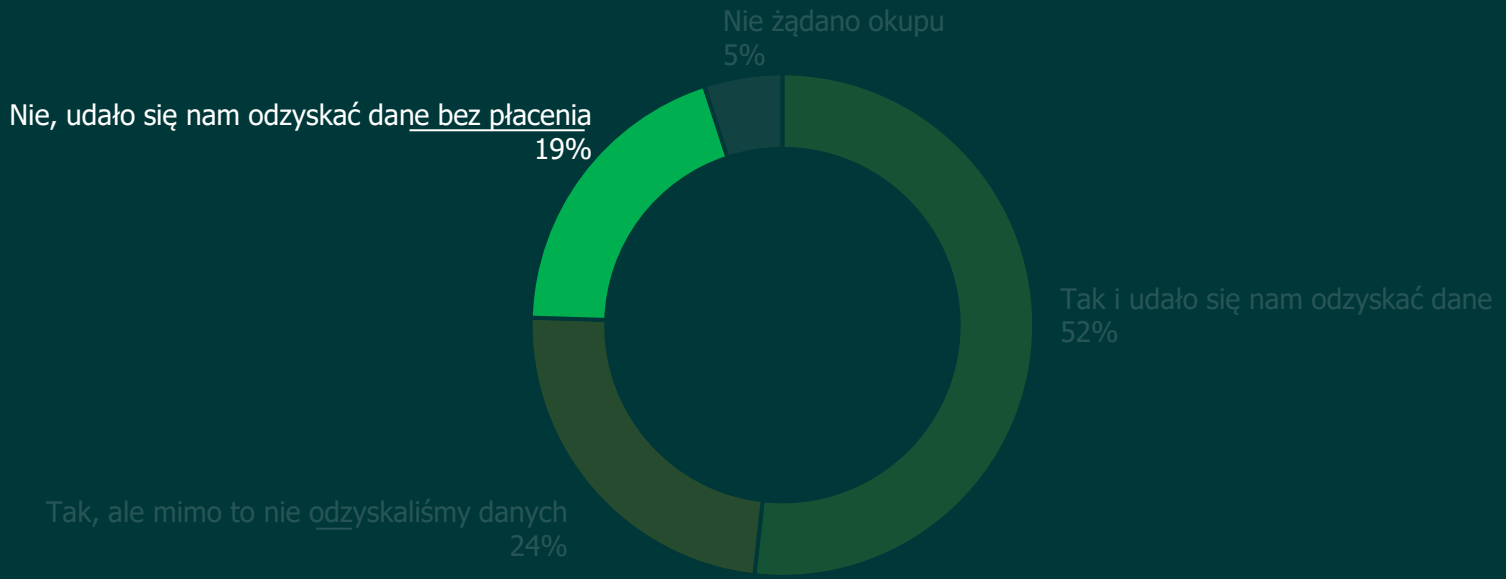
Czy Państwa firma zapłaciła okup w celu odzyskania danych?



Źródło: Raport nt. trendów w ransomware w 2022 r.
https://vee.am/RW22

Okup ≠ działanie naprawcze

Czy Państwa firma zapłaciła okup w celu odzyskania danych?



Źródło: Raport nt. trendów w ransomware w 2022 r.
https://vee.am/RW22

VEEAM

Potwierdzona niezmienność w każdym miejscu

VEEAM READY Repository
VEEAM READY Object
VEEAM READY Object with Immutability

Scale-out Backup Repository

Warstwa wydajności

DAS

NAS

Urządzenie deduplikujące

Wzmocnione repozytorium

Niezmienność w każdym miejscu

- Na podstawie zasad
- Transparentność
- Oszczędność miejsca
- Samowystarczalność
- Brak dodatkowych kosztów

Warstwa pojemności

Zgodne z S3

Obiektowa pamięć masowa IBM

Google Cloud Platform

Amazon S3

Microsoft Azure Blob Storage

Warstwa archiwizacji

Amazon S3 Glacier

Microsoft Azure Archive Blob Storage

Najlepsze praktyki z zakresu ochrony przed atakami ransomware

3

Trzy różne egzemplarze danych

2

Dwa różne nośniki

1

Jeden egzemplarz w lokalizacji zewnętrznej

VEEAM

1

W tym:
offline z separacją fizyczną
lub gwarantowaną niezmiennością

0

Brak błędów po automatycznych testach kopii zapasowych i weryfikacji odzyskiwania

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

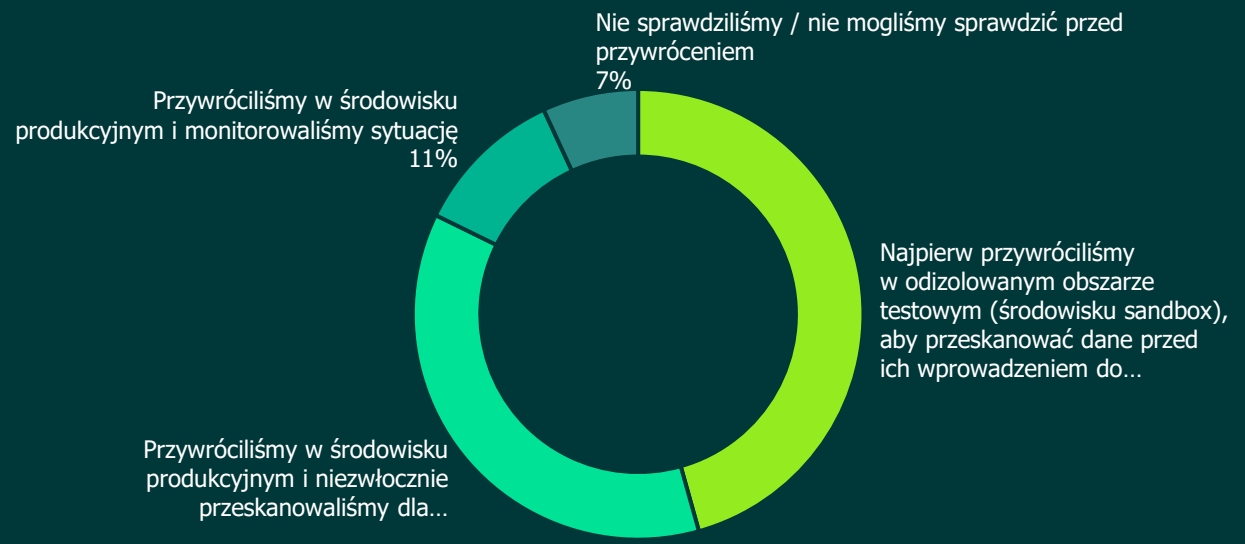
Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

Działania naprawcze: przywracanie „czystych” danych

46%

firm chcących odzyskać dane po ataku ransomware najpierw przywróciło je w odizolowanym środowisku testowym

Jak Państwo sprawdzili, czy dane systemów / kopie zapasowe były „czyste”, zanim zostały przywrócone? (n=555)

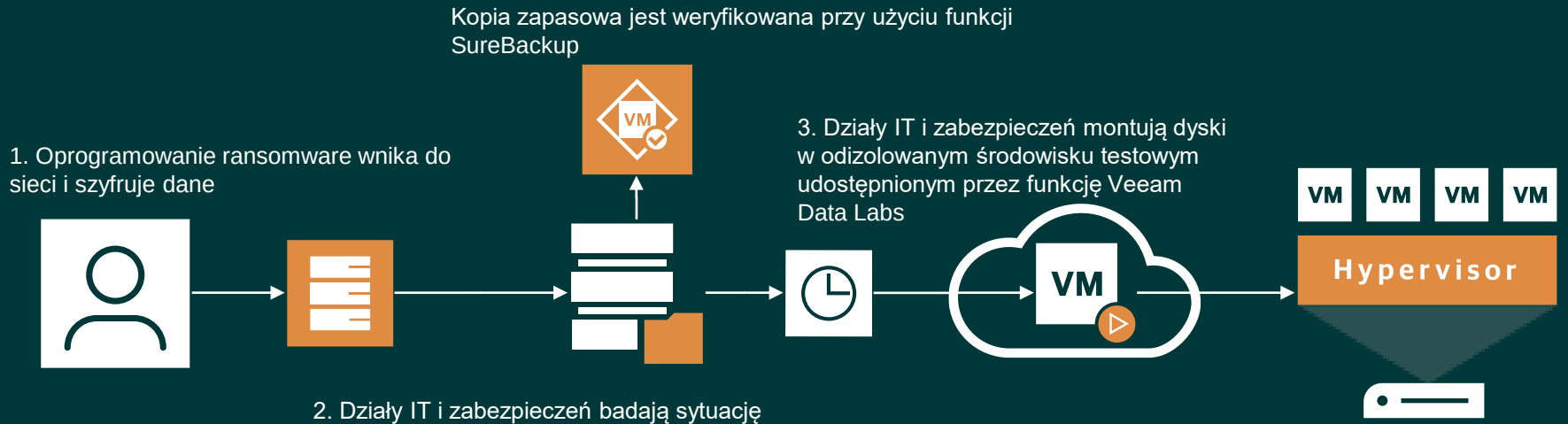


Źródło: Raport nt. trendów w ransomware w 2022 r.
https://vee.am/RW22

VEEAM

Przywracanie etapowe

Funkcja dająca pewność, że dane przeznaczone do przywrócenia do środowiska produkcyjnego nie zawierają złośliwego oprogramowania



Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Odzyskiwanie na dużą skalę

Atak ransomware to katastrofa

Ustalenie zasięgu

Ocalałe repozytoria

Przywracalne „czyste” dane

Odzyskiwanie do alternatywnej infrastruktury

Ochrona przed atakami ransomware

Bezpieczne **kopie zapasowe** to ostatnia linia **obrony**

Backup

- Potwierdzona niezmienność
- Weryfikacja kopii zapasowych
- Reguła 3-2-1-1-0

Odzyskiwanie

- Natychmiastowe odzyskiwanie na dużą skalę
- Bezpieczne przywracanie
- Orkiestracja odzyskiwania po awarii

Rozwiązanie definiowane programowo, bez uzależnienia od zastrzeżonego sprzętu

VEEAM

Natychmiastowe odzyskiwanie na dużą skalę

General options

- File-level recovery (Windows)
- V2V conversion to vSphere/ Hyper-V
- Full VM restore
- VM files restore
- Multi-VM Instant Recovery
- VM hard disk restore
- Failover to a replica VM
- File-level recovery (Multi-OS)
- Quick Rollback
- U-AIR restore
- Restore from a replica VM
- Replicate VM from a backup
- Instant VM disk recovery
- Staged Restore
- Secure Restore
- Data Integration API
- Instant first-class disk recovery
- Instant DB recovery

Veeam Explorers

Active Directory
- Export container/ object
- Restore system objects/GPO
- Restore a deleted container/ object
- Restore a changed container/ object

Exchange
- Save data
- Send data
- Restore folder/ item/mailbox
- Export to PST file

Teams
- Save file/as ZIP
- Send post/file
- Restore team/ channel/tab/ post/file
- Export post

SharePoint
- Save library/ document
- Send library/ document
- Restore library/list/ document/site
- Export library

OneDrive
- Save folder/ document
- Send document
- Restore folder/ document
- Copy data to same/ different user

Oracle
- Restore the latest state
- Restore to a specific point in time
- Restore to a specific transaction
- Restore from Oracle RMAN backup

SQL
- Restore the latest point
- Restore to specific time/ transaction
- Restore/ export DB schema
- Export latest or point-in-time state
- Publish latest or point-in-time state
- Export as MDF/BAK

Agents

- Agent Backup to a Hyper-V VM
- Guest OS files/ folders/ volumes
- Agent Linux
- Agent Windows
- Agent Mac
- Export a point as a virtual disk
- P2C conversion
- Application-level restore

Network Shares

- Restore entire file share
- Rollback to a point in time
- Restore files and folders
- Restore permissions and security attributes
- Instant share publishing

91

VEEAM

Recovery scenarios with Veeam Backup & Replication v11

Backup Enterprise Manager

- 1-click VM/file restore
- Virtual disk restore
- Launch failover plan
- Restore of vCD infrastructure
- Exchange item restore
- SQL/Oracle DB restore
- Self-service Restore Portal
- Restore via RESTful API

vCloud Director

- Instant VM Recovery into vApp/vSphere
- Full restore into vApp/ vSphere
- vCloud vApp restore
- Linked Clone VMs to vCD

Tape

- Full VM to infrastructure
- Files from tape
- Backup from tape
- Tenant restore

Extra

- Restore via PowerShell
- Extract utility
- File restore audit
- Restore under user context

Cloud

- Partial/full site failover
- Restore to Azure VM/ AWS EC2
- Restore from "deleted" VCC backups
- Restore from object storage
- Restore from the VCC Provider
- C2V conversion via "external" repo

Explorer for Storage Snapshots

- Guest files (Windows/ Multi-OS)
- Instant VM/disk Recovery
- SQL/Oracle DB restore
- Exchange/SP/ AD item restore

Atak ransomware to katastrofa

Atak ransomware to katastrofa

Pewność odzyskania obciążenia

Czy masz niezawodne kopie danych na potrzeby odzyskiwania?

Kopie zapasowe o zweryfikowanej odzyskiwalności

Odzyskiwanie na dużą skalę

Jak możesz skrócić rzeczywisty czas odzyskiwania?

Zorkiestrowane procesy robocze

Ustalenie zasięgu

Jaki jest zasięg?

Ocalałe repozytoria

Czy zostały jakieś egzemplarze?

Przywracalne „czyste” dane

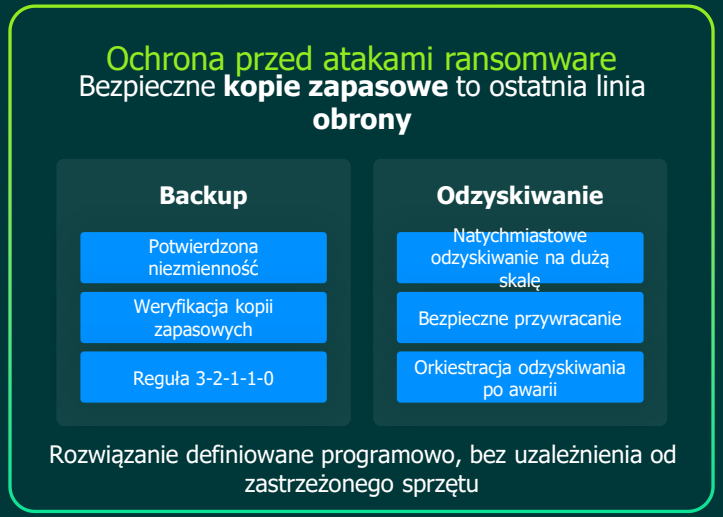
Czy są bezpieczne?

Odzyskiwanie do alternatywnej infrastruktury

Czy jesteś w stanie zacząć od zera?

W chmurze hybrydowej lub między platformami

Nie musisz płacić okupu!



Ogranicz ryzyko utraty danych przez monitorowanie w czasie rzeczywistym, aby neutralizować problemy, zanim przerodzą się w zagrożenia dla środowiska

Chroń dane przy użyciu bezpiecznej pamięci masowej i zweryfikowanych kopii zapasowych

Odzyskuj dane szybko i niezawodnie bez ponownego wprowadzania zagrożeń czy płacenia okupu

VEEAM

Dziękujemy

VEEAM