VECTOR® SOLUTIONS | BE ABLE

We integrate Hybrid IT solutions. Together

vectorsolutions.net

Bunkier dla danych

Czyli jak zabezpieczyć Backup przed Ransomware?

Łukasz Wasielewski
Solution Manager – Cloud & IT Infrastructure

RANSOMWARE W POLSCE

Komenda Wojewódzkiej
Państwowej Straży Pożarnej w Łodzi

**Atak na serwer WWW,
zaszyfrowane dane z żądaniem okupu**

Urząd Gminy
w Lututowie

**Atak na infrastrukturę,
zaszyfrowane dane z żądaniem okupu**

Urząd Gminy
Kościerzyna

Cyberprzestępcy dostali się do sieci, z której korzystają wszystkie jednostki organizacyjne podlegające do Urzędu Gminy Kościerzyna, zaszyfrowali wszystkie dane, Hakerzy żądają okupu w kryptowalucie

Urząd Marszałkowski
Województwa Małopolskiego

**Atakujący zażądał zapłaty okupu,
utracone dane**

Instytut Centrum Zdrowia Matki Polki

Szczególnie bolesny atak dla możliwości operacyjnych jednego z najważniejszych szpitali w Polsce

**Koszt ataku dla polskich firm
to średnio 1,49 mln zł – ustalił Sophos**

DYREKTYWA NIS 2

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;

b) obsługę incydentu;

c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

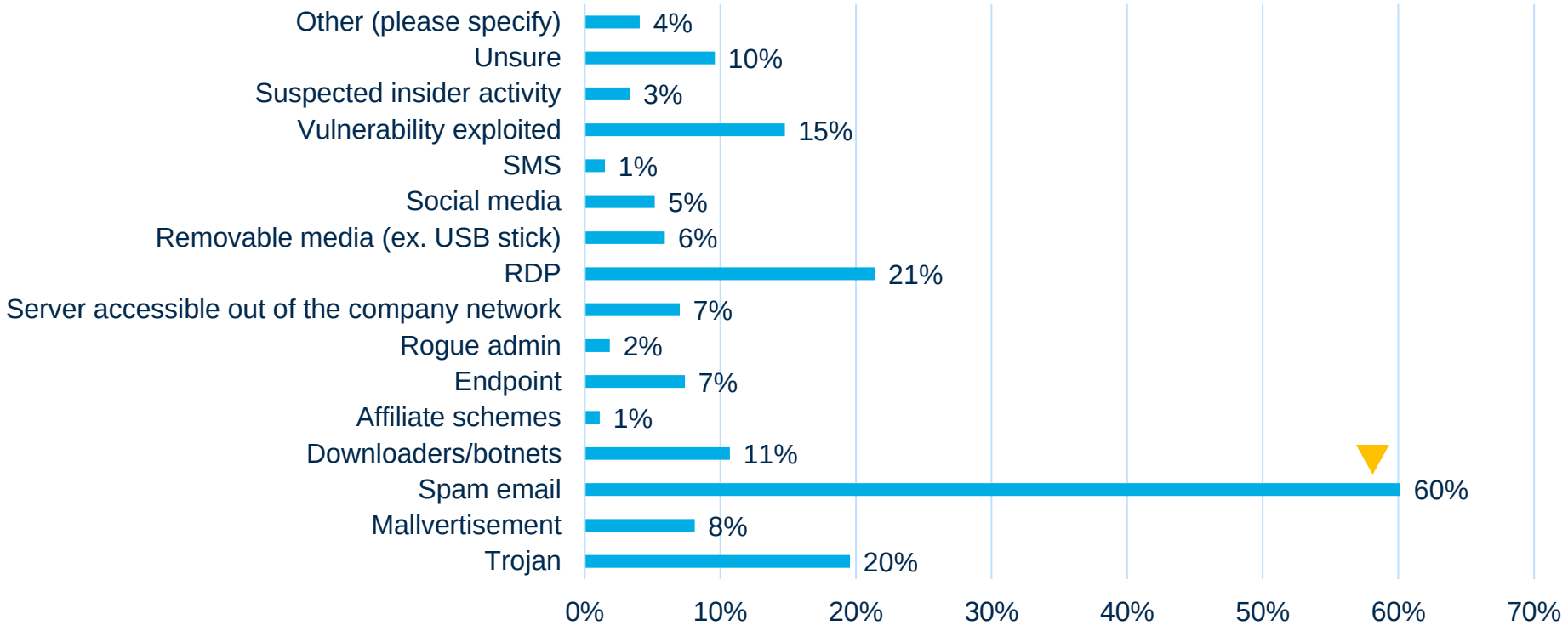
g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;

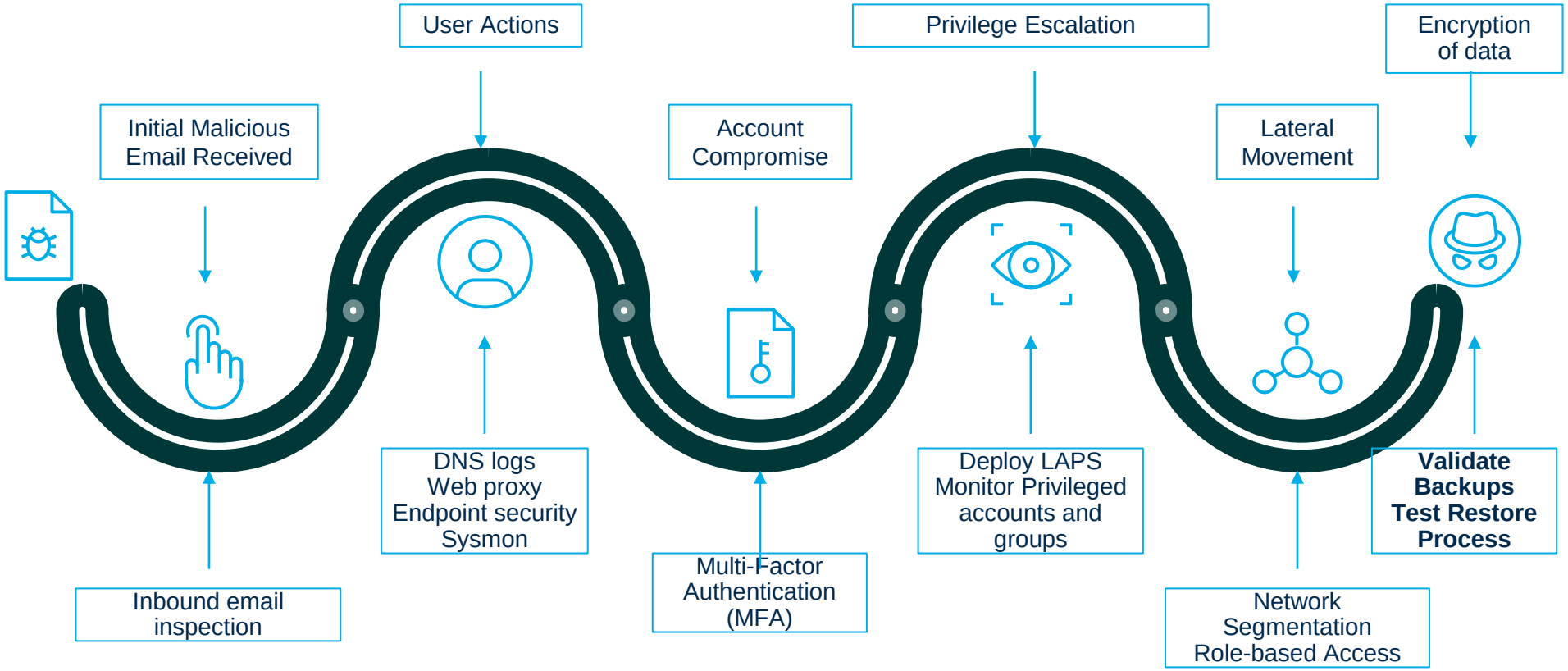
h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;

j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Skąd bierze się ransomware?




Initial Malicious Email Received
User Actions
Account Compromise
Privilege Escalation
Lateral Movement
Encryption of data
Inbound email inspection
DNS logs
Web proxy
Endpoint security
Sysmon
Multi-Factor Authentication (MFA)
Deploy LAPS
Monitor Privileged accounts and groups
Network Segmentation
Role-based Access
Validate Backups
Test Restore Process

Jak uniknąć usunięcia danych?

T1485 Data Destruction

https://attack.mitre.org/techniques/T1485/

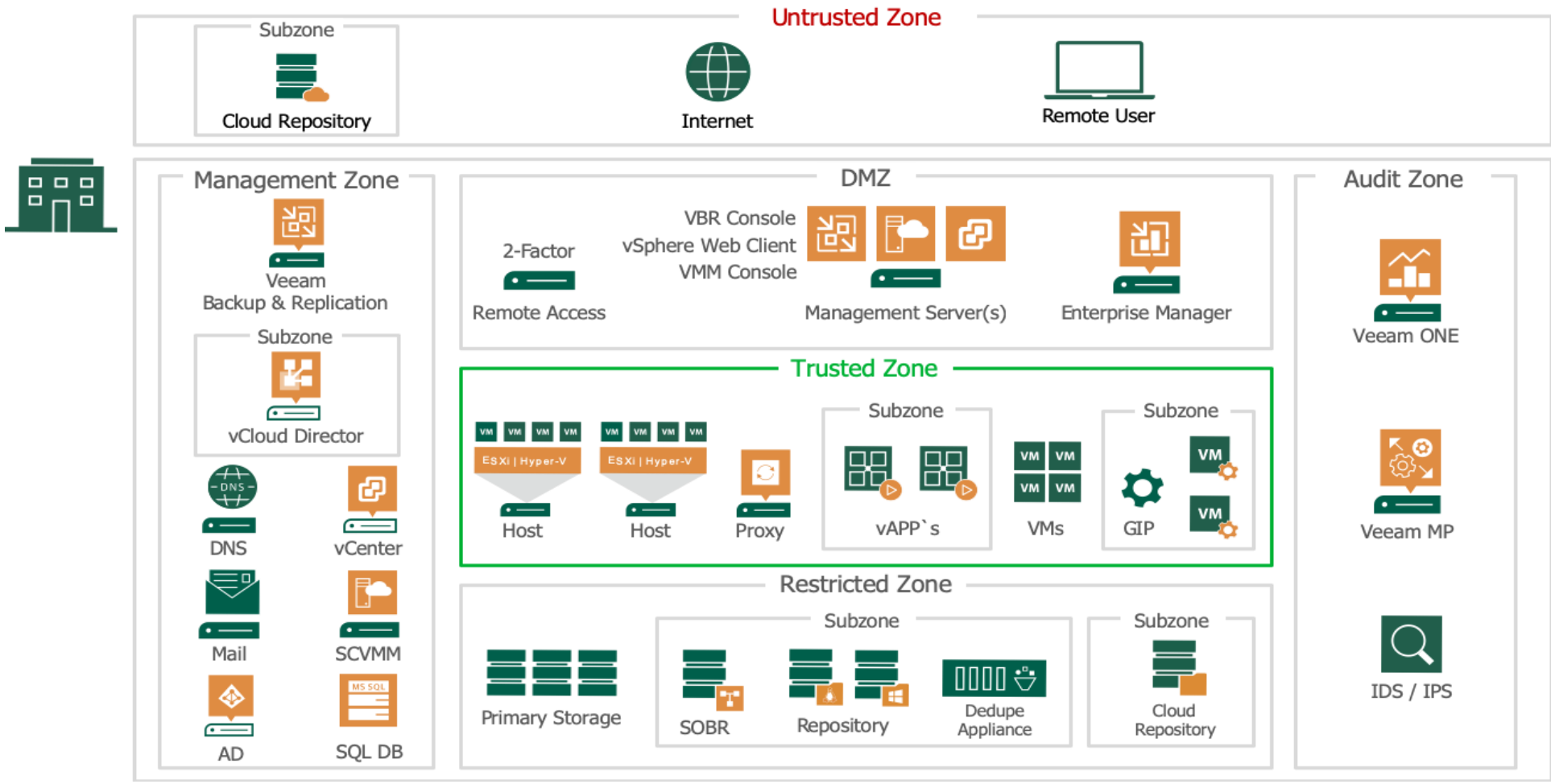
Three different copies of data

Two different media

One offsite copy

Of which is:
offline air-gapped or immutable

No errors after automated backup testing & recoverability verification

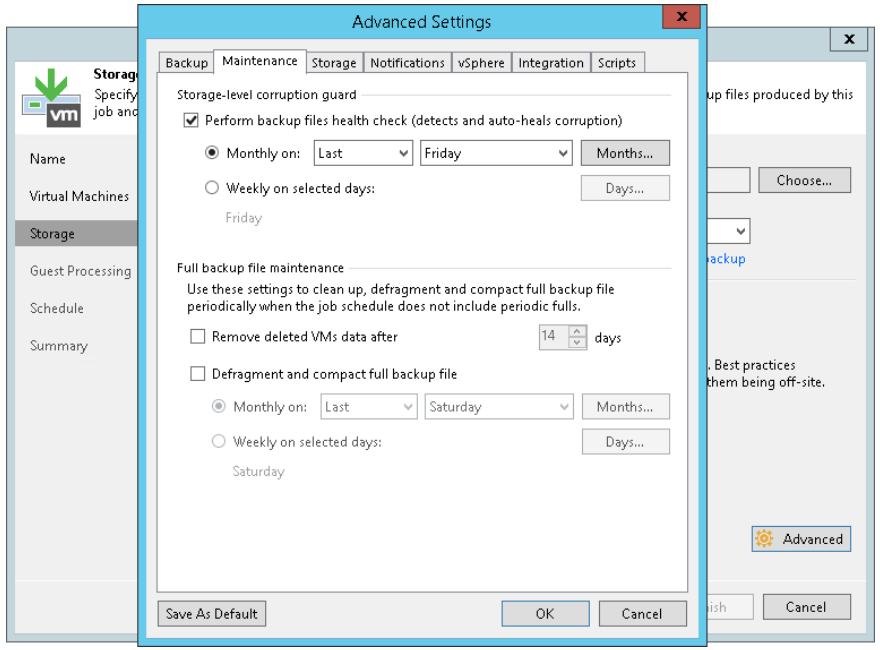

Untrusted Zone
Subzone
Cloud Repository
Internet
Remote User
Management Zone
Veeam
Backup & Replication
Subzone
vCloud Director
DNS
vCenter
Mail
SCVMM
AD
SQL DB
DMZ
2-Factor
Remote Access
VBR Console
vSphere Web Client
VMM Console
Management Server(s)
Enterprise Manager
Trusted Zone
ESXi | Hyper-V
ESXi | Hyper-V
Host
Host
Proxy
Subzone
vAPP`s
VMs
Subzone
GIP
Restricted Zone
Primary Storage
Subzone
SOBR
Repository
Dedupe
Appliance
Subzone
Cloud
Repository
Audit Zone
Veeam ONE
Veeam MP
IDS / IPS

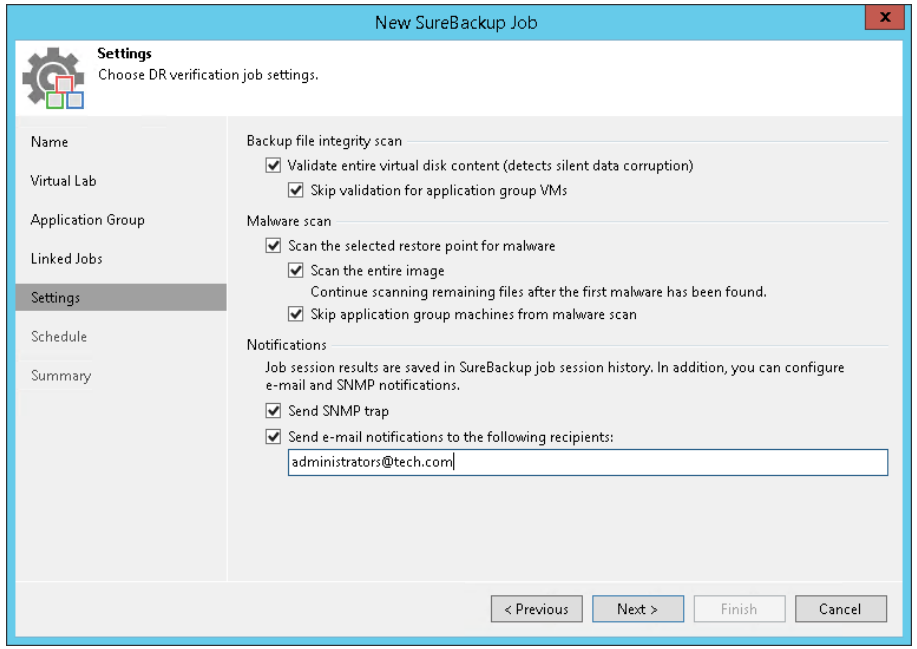
Jak uniknąć uszkodzenia danych backupowych?

T1561 Disk Wipe/Corruption

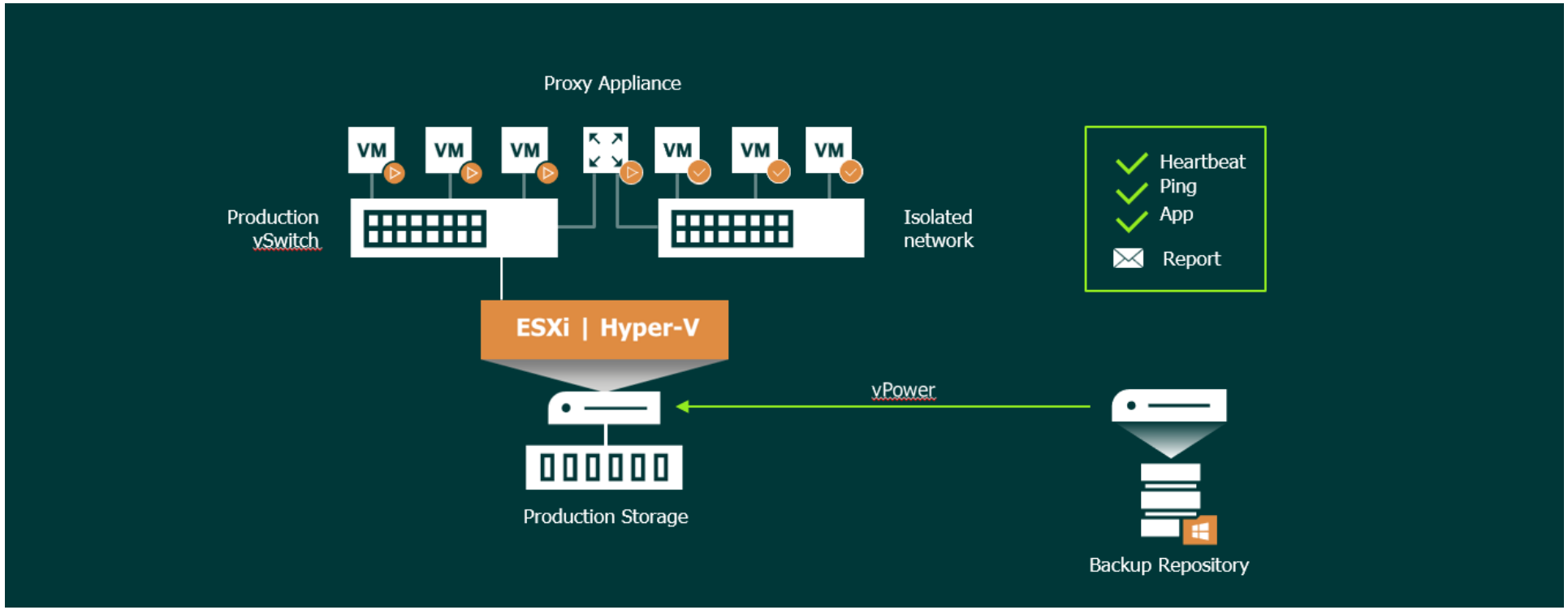
https://attack.mitre.org/techniques/T1561/

SURE BACKUP





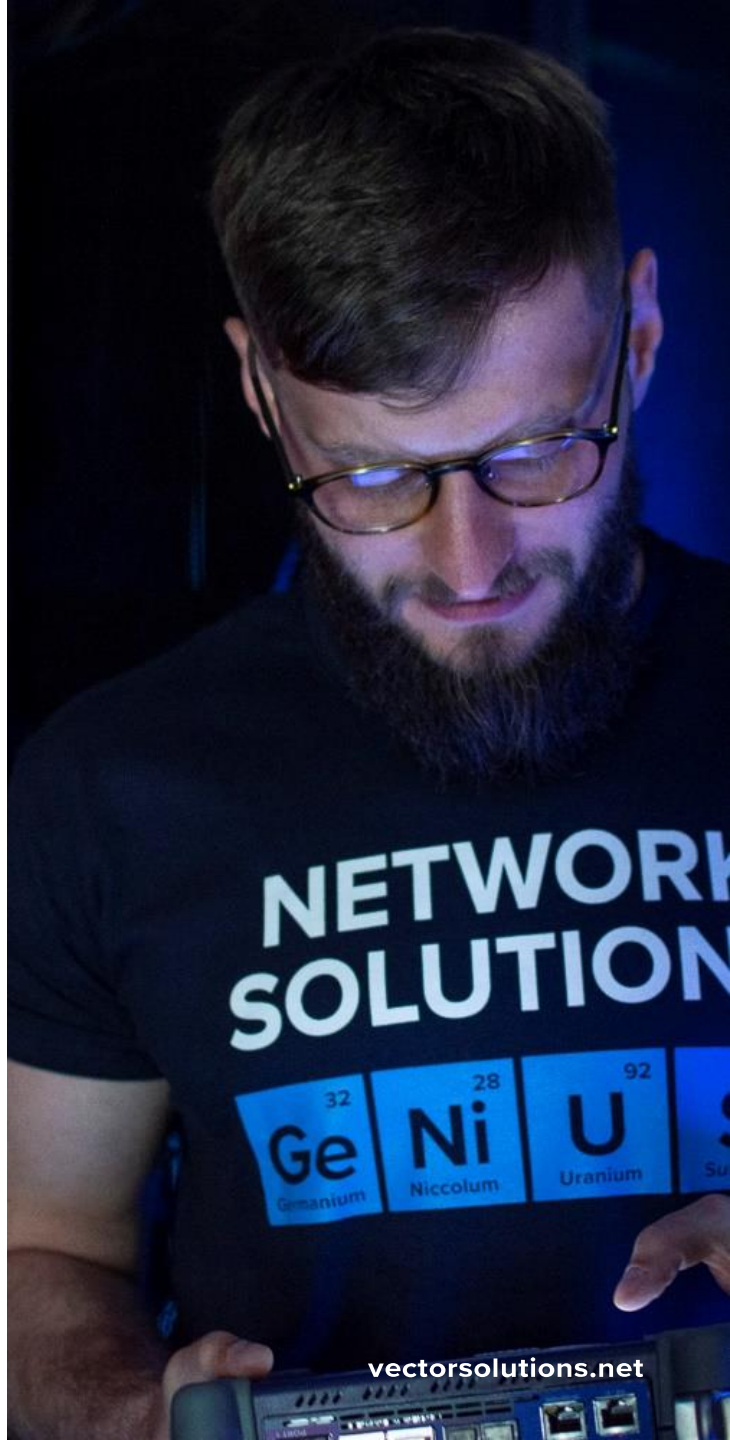
HEALTHCHECK


Proxy Appliance
VM
VM
VM
VM
VM
VM
Production
vSwitch
Isolated
network
Heartbeat
Ping
App
Report
ESXi | Hyper-V
vPower
Production Storage
Backup Repository

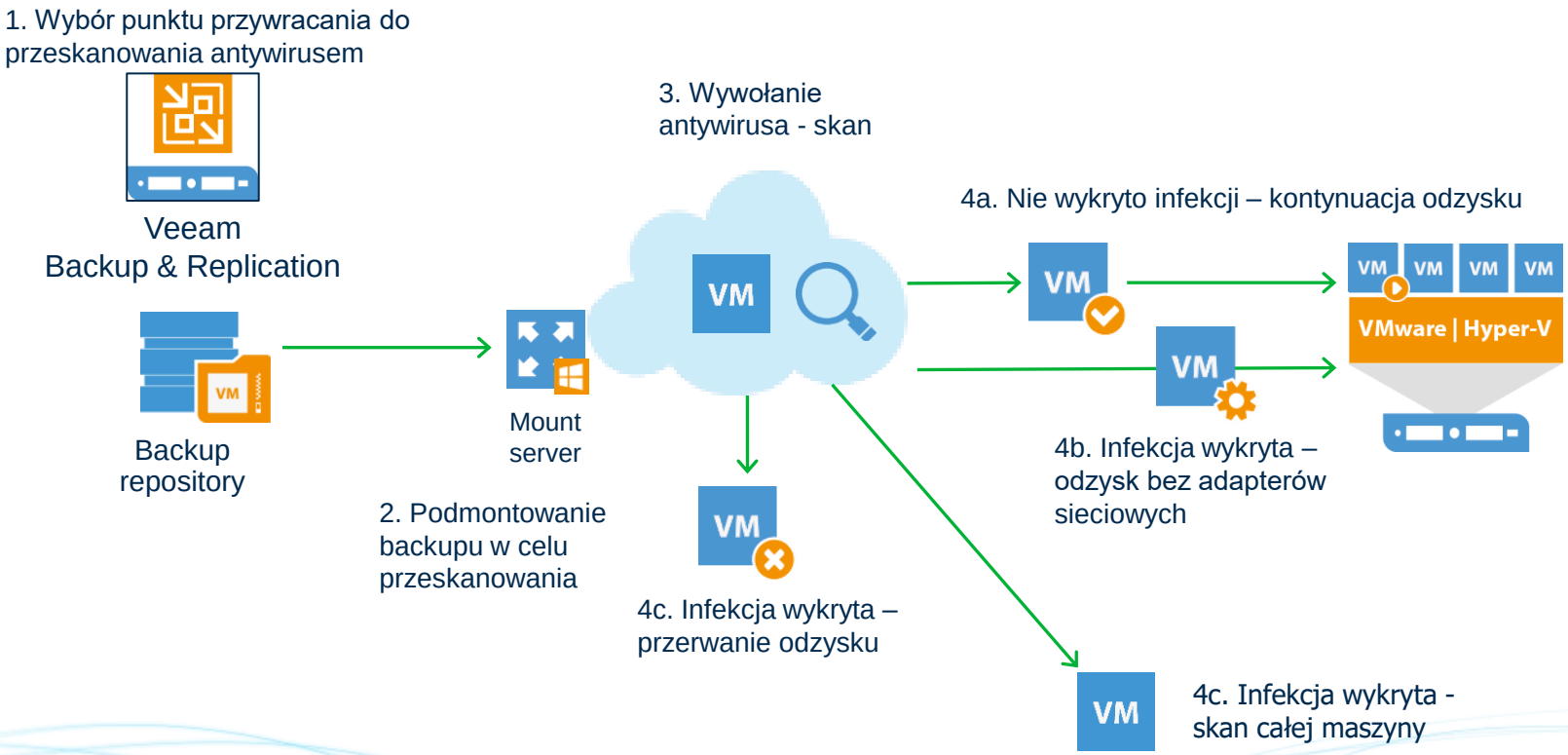
Co w przypadku zaszyfrowania danych produkcyjnych?

T1486 Data Encrypted for Impact

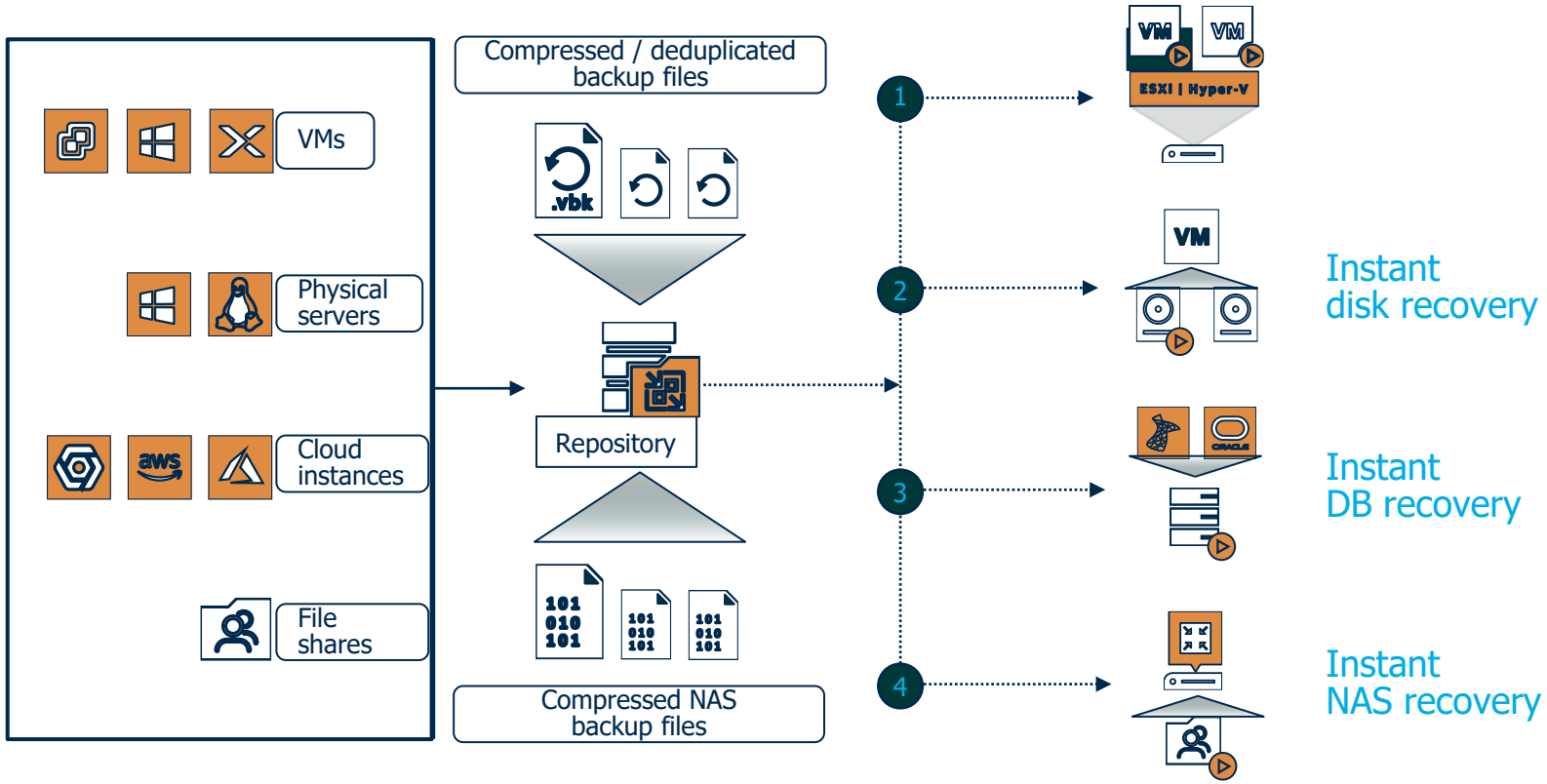
https://attack.mitre.org/techniques/T1486/



SECURE RESTORE



INSTANT RECOVERY

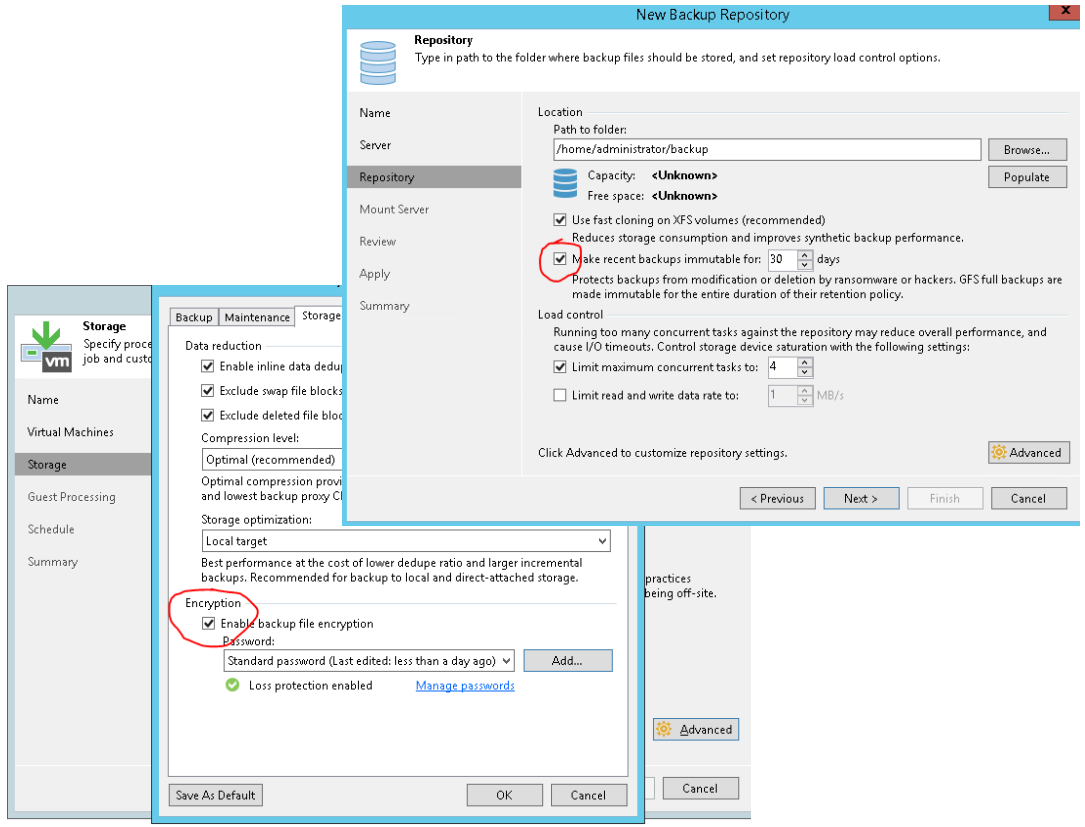


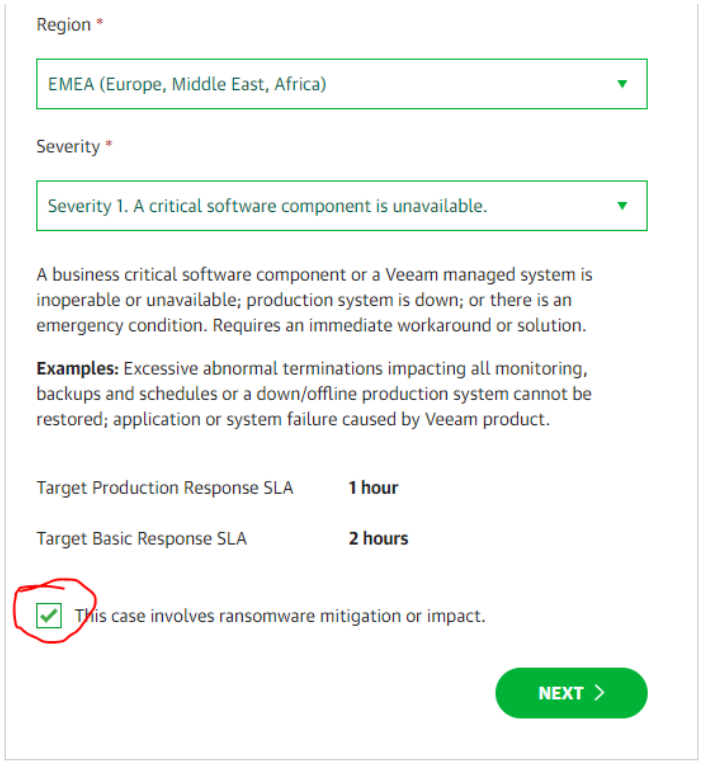
Jak się przygotować na atak?

T1490 Inhibit System Recovery

https://attack.mitre.org/techniques/T1490/

CO ZROBIĆ PRZED? I CO ZROBIĆ PO?





Lokalne referencje

LUBELSKIE CENTRUM
INNOWACJI I TECHNOLOGII

Instytucja Samorządu
Województwa Lubelskiego

Zakres kompleksowej modernizacji i podniesienia funkcjonalności obejmował

- analizę potrzeb i wybór rozwiązania adresującego potrzeby klienta
- rozwój środowiska w ramach oprogramowania Veeam Backup & Replication, testowanie i konfigurację
- szkolenie z zakresu administracji i zarządzania systemem
- wsparcie techniczne poprzez utrzymanie i rozwój wdrożonej platformy

W LCIiT rozwiązaniem backupowym zaopiekowano infrastrukturę sprzętową opartą o serwery, macierze, a także środowisko wirtualne Vmware vSphere w wersji 6.7 zawierające **łącznie 250 maszyn wirtualnych oraz 1600 użytkowników usługi Microsoft 365.**

VECTOR SOLUTIONS

OSTATNIE PROJEKTY:

Dostawa i uruchomienie klastra Firewalli NGFW Checkpoint Maestro, wraz z ochroną urządzeń końcowych Harmony Endpoint i usługami SASE Harmony Connect

DLA: Dużego operatora telkomunikacyjnego

Dostawa i wdrożenie sieci automatycznej opartej na rozwiązaniu Cisco SDA wraz z wdrożeniem polityki bezpieczeństwa sieci ZTNA i kontrolą dostępu do sieci NAC

DLA: Jednostki publicznej szczebla wojewódzkiego

Dostarczenie klastra macierzy dyskowych IBM FlashSystem 7300 replikujących się między dwoma centrami danych o pojemności skutecznej 500TB dla współdzielonych usług IT

DLA: Warszawskiego operatora usług Data Center

Projekt, dostawa i konfiguracja trzypoziomowej fabryki przełączającej wykorzystującej standard BGP EVPN dla Data Center na bazie przełączników i routerów Huawei

DLA: Ogólnopolskiego operatora usług Data Center

Dostawa i konfiguracja firewalli Palo Alto wraz z oprogramowaniem Panorama, wdrożenie polityki bezpieczeństwa sieciowego wsparcie serwisowe

DLA: Publicznej jednostki ratownictwa medycznego

OPINIE KLIENTÓW:

„W przypadku usług IT niezbędni są zarówno dostawcy, jak i sprawdzony partner biznesowy, który przeprowadza wdrożenie, trasfer wiedzy oraz wspomaga instytucje w zarządzaniu oprogramowanie. Współpracujemy z VECOTR SOLUTIONS i jest to bardzo dobry partner, certyfikowany w zakresie rozwiązań, których używamy.”

Robert Targos

Zastępca Dyrektora, LCIT

„Jesteśmy zadowoleni z przebiegu współpracy. Zamówienie zostało zrealizowane w ustalonym terminie, a dostarczony sprzęt spełnia wymagania jakościowe. Inżynierowie VECTOR SOLUTIONS wykazali się profesjonalizmem i zorientowaniem na potrzeby Klienta, a także służą pomocą i wiedzą w zakresie dostarczonych rozwiązań.”

Paweł Sokołowski

Dyrektor Pionu urządzeń konsumenckich, Cyfrowy Polsat

„Zdecydowaliśmy się na współpracę z VECTOR SOLUTIONS ze względu na dobre doświadczenia związane z tym integratorem. Gwarantuje on rzetelne i profesjonalne podejście, a także zastosowanie urządzeń, które rzeczywiście będą wspierać nasz biznes”

Radosław Potera

CTO, Atman

REFERENCJE:

UNIWERSYTET MEDYCZNY W ŁODZI

NETIA

CANAL+

NASK

Łódzki Urząd Wojewódzki w Łodzi

HUAWEI Enterprise Partner VAP

veeAM PROPARTNER Gold Reseller

DELL

rubrik

CHECK POINT™

f5

Hewlett Packard Enterprise

IBM

paloalto® NETWORKS

vectorsolutions.net

VEEAM

PROPARTNER
Gold Reseller

rubrik

Kontakt

ŁUKASZ WASIELEWSKI
Solution Manager - Cloud & IT Infrastructure

M +48 600 308 275

E l.wasielewski@vector.net

We integrate Hybrid IT solutions. Together

Poznaj szczegóły

vectorsolutions.net

vectorsolutions.net