Cyfrowy Bunkier Dell Technologies

FORUM BEZPIECZEŃSTWA BANKÓW, ZBP

Paweł Chruściak
Dell Technologies
pawel.chrusciak@dell.com

DELL EMC

Dell Customer Communication - Confidential

Strategia ochrony w organizacjach:

- **Budowa Twierdzy** (Strategia bezużyteczna w przypadku danych zaszyfrowanych)
  - Próba niedopuszczenie do zainfekowania danych
  - Firewall'e
  - Monitorowanie użytkowników
- **Cyfrowy Bunkier**
  - Założenie, że skuteczny atak może nastąpić
  - Przywrócenie na moment sprzed ataku

DELL Technologies

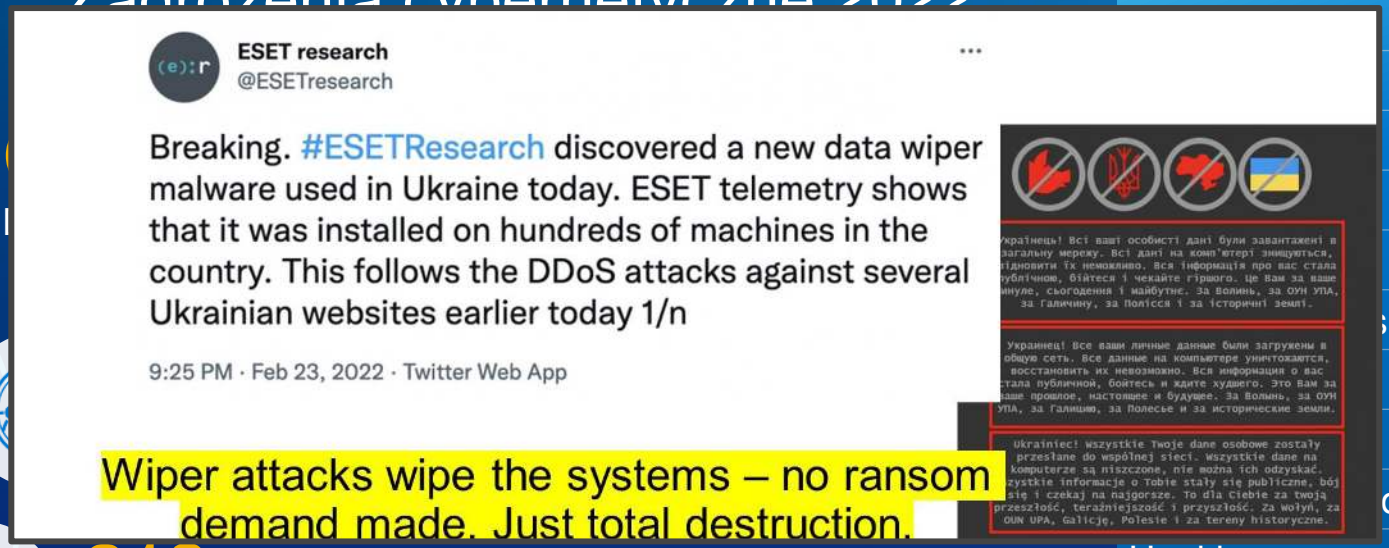
Dell Customer Communication - Confidential

Główne Funkcje Cyfrowego Bunkra

1. Zapewnienie gwarancji bezpieczeństwa kluczowych danych
2. Wykrywanie skutecznych ataków cyfrowych
3. W przypadku ataku zminimalizowanie czasu odtworzenia

DELL Technologies

Zagrożenia cybernetyczne 2022



$13m

Średni koszt dla organizacji po skutecznym cyberataku

Średni czas wykrycia skutecznego ataku to 233 dni

Banking	$18.4M
	$17.8M
	$16.0M
	$15.8M
	$15.8M
	$14.7M
	$13.9M
	$13.8M
	$13.7M
ds	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

[2]Cybersecurity Ventures: *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021*

[3]Accenture Insights, Ninth Annual Cost of Cyber crime Study March , 2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[4]Varonis,2021 https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

Dell Customer Communication - Confidential

Cyfrowy Bunkier to dopowiedź na szerokie spektrum cyberzagrożeń

Przestępstwo

Kradzież i wymuszenia finansowe, korzyści

Insider

Zaufani insiderzy kradną lub wymuszają z powodów osobistych, finansowych i ideologicznych.

Mają uprzywilejowany dostęp do systemów

Szpiegostwo

Podmioty korporacyjne lub państwowe kradną cenne dane

Haktywizm

Przyczyny polityczne lub społeczne

Terroryzm

Sabotaż i zniszczenie w celu zaszczepienia strachu

Wojna

Podmioty państwowe z bronią cybernetyczną (NotPetya)

Dell Customer Communication - Confidential

Dyrektywa EU

Network and Information Security – rev 2 (NIS 2)

zmiany i szanse

Historia i zakres NIS – „pierwsze wydanie”

2016 – przyjęcie dyrektywy NIS (Network and Information Security)
2018 – Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC - polska implementacja NIS)

Na bazie KSC powstały w Polsce:

- Rządowe Centrum Bezpieczeństwa – RCB
- CSIRT (Computer Security Incident Response Team) poziomu krajowego – GOV, MON, NASK, KNF
- CSIRT komercyjne – EY, NETIA,……

Zdefiniowano Dostawców Usług Cyfrowych - zaliczamy do nich: internetową platformę handlową, wyszukiwarkę internetową lub usługę przetwarzania w chmurze

Rząd stworzył i opublikował w formie Rozporządzenia Rady Ministrów Wykaz Usług Kluczowych - https://dziennikustaw.gov.pl/D2018000180601.pdf

Dell Customer Communication - Confidential

Przyszłość i zakres NIS2

Od daty wejścia w życie Dyrektywy, czyli 16 stycznia 2023 r., Państwa Członkowskie UE mają 21 miesięcy na wprowadzenie postanowień Dyrektywy do prawa krajowego. W Polsce oznacza to konieczność nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, co powinno nastąpić najpóźniej do 17 października 2024 roku.

NIS	NIS2
Sektory objęte dyrektywą	**Rozszerzony zakres obejmujący więcej sektorów i usług jako kluczowe lub ważne podmioty**
Ochrona zdrowia	Dostawcy publicznych sieci lub usług komunikacji elektronicznej
Transport	Usługi cyfrowe świadczone przez platformy sieci społecznościowych i centra danych
Infrastruktura bankowa i rynków finansowych	Zarządzanie wodą i ściekami
Infrastruktura cyfrowa	Przestrzeń kosmiczna
Wodociągi	Produkcja niektórych krytycznych produktów np. farmaceutyków, urządzeń medycznych i chemikaliów
Energetyka	Usługi pocztowe i kurierskie
Dostawcy usług cyfrowych	Żywność
	Administracja publiczna

- Gospodarowanie odpadami
- Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne sprzęt elektryczny, maszyny i wyposażenie, pojazdy samochodowe, przyczepy i naczepy, inny sprzęt transportowy)
- Produkcja i dystrybucja chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Dostawcy cyfrowi

DELL Technologies

DELL Technologies

CyberAtaki to obecnie największe zagrożenie dla biznesu, większe od terroryzmu, klęsk żywiołowych czy baniek finansowych

Paul Mee & Till Schuermann

- Harvard Business Review

Disaster Recovery to nie Cyber Recovery

Disaster Recovery / Business Continuity to za mało żeby zabezpieczyć się przed aktualnymi cyber-zagrożeniami

DELL Technologies

Dell Customer Communication - Confidential

Generyczny scenariusz ataku

Narzędzia / działania reaktywne

Działania proaktywne / procesy / procedury

Rozpoznanie

Phishing lub exploit

Ustanowienie przyczółka

Rozszerzenie wpływu

Dywersja

Cel – krytyczne systemy i kopie zapasowe

Atak

Prewencja i monitorowanie

Wykrywanie skutecznego ataku i odpowiedź

Odtworzenie

Szybsza reakcja zmniejsza zasięg i skraca czas wykrywania skutecznego ataku

Copyright © Dell Inc. All Rights Reserved.

Cyfrowy Bunkier

Ochrona przed ransomware/hacker

Izolacja

Fizyczna i logiczna separacja danych

Niezmienność

Blokada przed edycją lub skasowaniem danych. **Gwarancja niezmienności danych**

Weryfikacja

Analityka i wykrywanie ataków

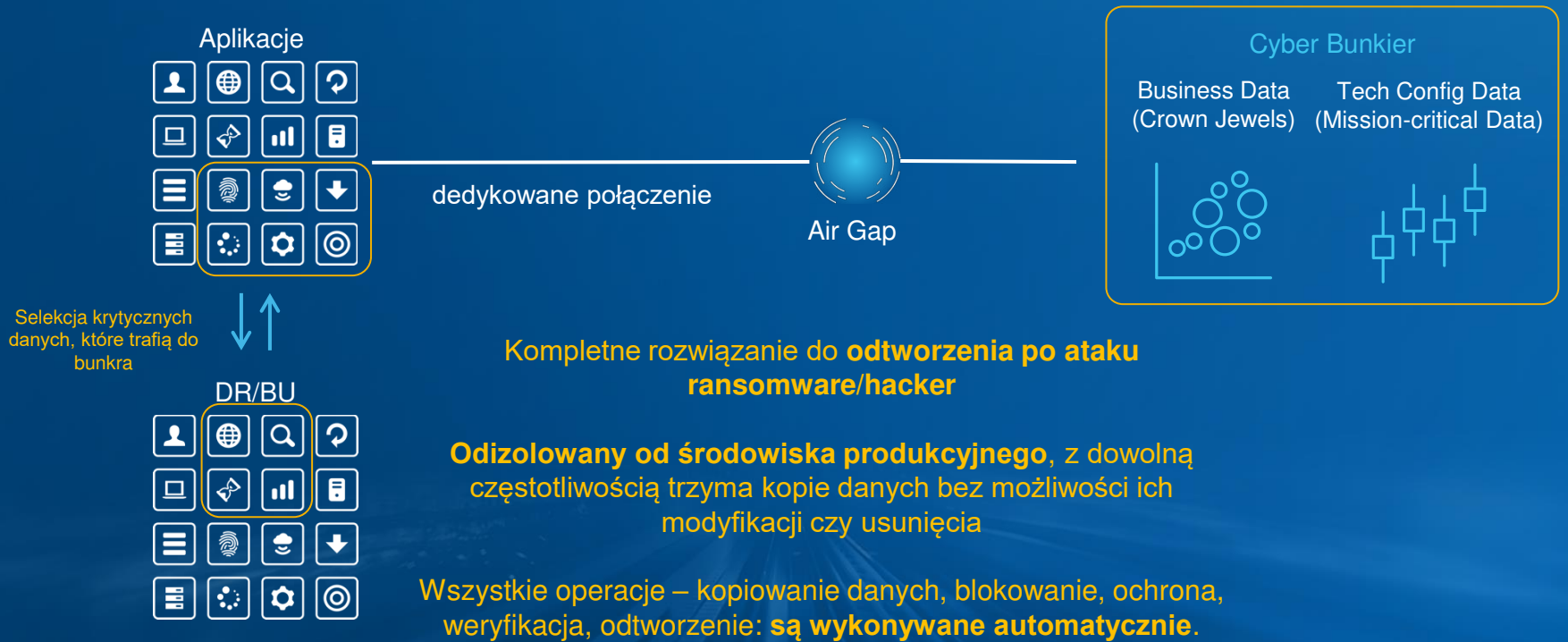
Procedury

Przetestowane metody odtworzenia danych

Dell Customer Communication - Confidential

Cyfrowy Bunkier

Krytyczne dane bezpieczne i odseparowane od sieci produkcyjnej



Kompletne rozwiązanie do **odtworzenia po ataku ransomware/hacker**

Odizolowany od środowiska produkcyjnego, z dowolną częstotliwością trzyma kopie danych bez możliwości ich modyfikacji czy usunięcia

Wszystkie operacje – kopiowanie danych, blokowanie, ochrona, weryfikacja, odtworzenie: **są wykonywane automatycznie**.

Dell Customer Communication - Confidential

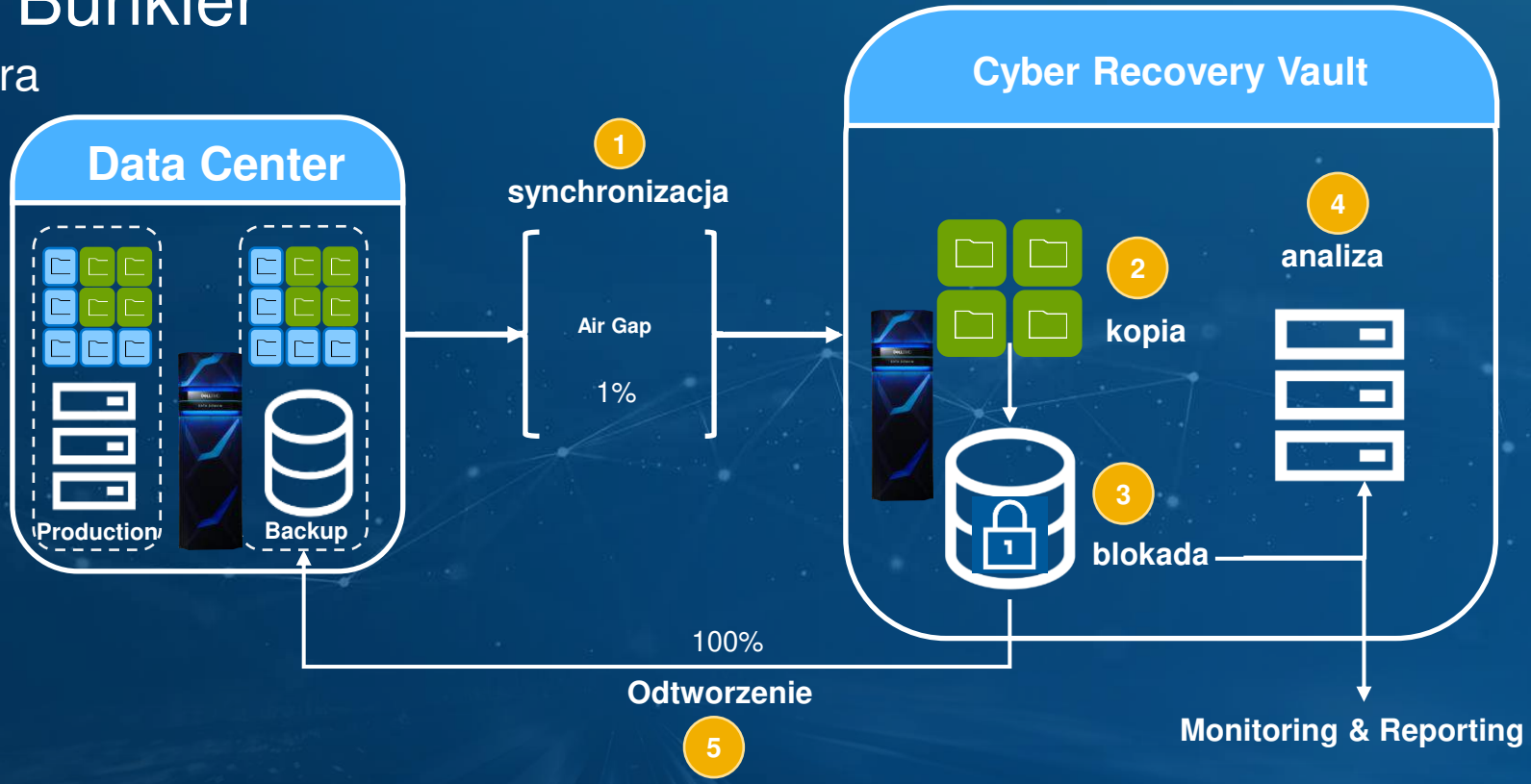
Jak zbudować Cyber Bunkier?
architektura

DELL Technologies

Dell Customer Communication - Confidential

Cyber Bunkier

architektura



DELL Technologies

Dell Customer Communication - Confidential

Cyber Bunkier : receptura

- Trzecia kopia najważniejszych danych i konfiguracji systemów
- Pełna izolacja środowiska w bunkrze, poza momentem synchronizacji
- Dane w bunkrze zablokowane przed skasowaniem

„Cyfrowy Bunkier" składa się z następujących elementów:

- Dodatkowa kopia zapasowa na niezależnym urządzeniu Data Domain w bezpiecznej enklawie.
- Bezpieczna enklawa odtwarzania zabezpieczona fizycznie, monitorowana, izolowana.
- „Utwardzenie" urządzenia Data Domain w bezpiecznej eklawie odtwarzania oraz produkcyjnych urządzeń Data Domain
- „Air Gap", czyli automatyczne odcięcie komunikacji LAN/IP między produkcją a izolowaną enklawą
- Zablokowanie możliwości zmian na Data Domain - Retention Lock (Governance lub Compliance)
- Zapasowy serwer backupu w izolowanej enklawie odtwarzania
- Serwery aplikacji do odtwarzania testowego i weryfikacji danych w izolowanej enklawie odtwarzania
- Automatyzacja replikacja do bunkra
- Zbiór najlepszych praktyk stosowanych przy budowie izolowanej enklawy odtwarzania
- Usługi doradcze (analiza, klasyfikacja danych, projektowanie, tworzenie planów i polityk BC)
- Usługi implementacyjne (instalacja, konfiguracja, utwardzanie, testy, procedury odtwarzania i weryfikacji)
- Analityka (**CyberSense**)

DELL Technologies

Dell Customer Communication - Confidential

How CyberSense Works

Machine learning enables early detection & rapid recovery from a cyber attack

SECURITY ANALYTICS
100+ statistics indicative of cyber attack

COMPREHENSIVE INDEX
Changes in content over time

MACHINE LEARNING
Trained on thousands of trojans and 20+ attack vectors

Cyber Recovery with CyberSense

- Attack vector notification
- Ransomware
- Corrupted file details
- Data changes / deletions
- Breached user accounts
- Breached executables
- Recovery of last good copy

Internal Use - Confidential

DELL Technologies

Dell Customer Communication - Confidential

Compare: CyberSense vs. “Basic” Analytics

Machine learning enables early detection & rapid recovery within the Cyber Recovery vault

CyberSense:

Full content indexing of:

1. File metadata
2. Document metadata
3. Document content

vs.

Basic Analytics:

On-Premises Analytics Engine

1. Scans only file metadata

Cloud-based Analytics Engine

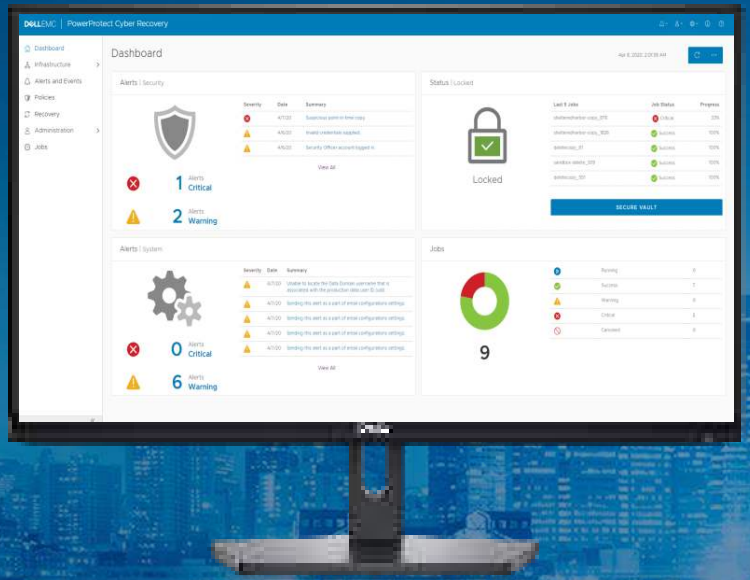
2
3

Suspicious files sent to cloud for 2nd pass or full content analysis

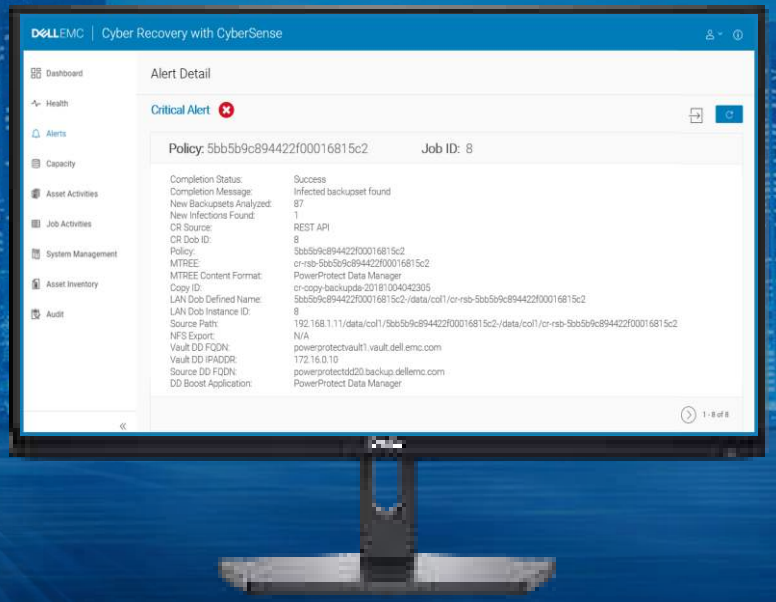
Internal Use - Confidential

DELL Technologies

PowerProtect Cyber Recovery



CyberSense Alert



DELL Technologies

Dell Customer Communication - Confidential

Strategia ochrony w organizacjach:

- **Strategia Twierdzy** (Strategia bezużyteczna w przypadku danych zaszyfrowanych)
  - Próba niedopuszczenie do zainfekowania danych
  - Firewall'e
  - Monitorowanie użytkowników
- **Strategia Cyfrowy Bunkier**
  - Założenie, że skuteczny atak może nastąpić
  - Przywrócenie na moment sprzed ataku

DELL Technologies

Dell Customer Communication - Confidential

Główne Funkcje Cyfrowego Bunkra

1. Zapewnienie gwarancji bezpieczeństwa kluczowych danych
2. Wykrywanie skutecznych ataków cyfrowych
3. W przypadku ataku zminimalizowanie czasu odtworzenia

DELL Technologies

1. Zapewnienie gwarancji bezpieczeństwa kluczowych danych

- Złota kopia
- Compliance / dane zamienione w kamień
- Niewidoczność
- Mamy pewność odtworzenia w przypadku ataku i destrukcji produkcji

Dell Customer Communication - Confidential

2. Wykrywanie skutecznych ataków cyfrowych

- Pełna weryfikacja danych produkcyjnych
- Codzienne upewnienie się, że nigdzie nie ma nawet fragmentu zaszyfrowanych danych
- W przypadku ataku, natychmiastowe wykrycie
- Ugaszenie pożaru gdy jest minimalny
- Wskazanie nieskompromitowanych, najbardziej aktualnych danych

DELL Technologies

Dell Customer Communication - Confidential

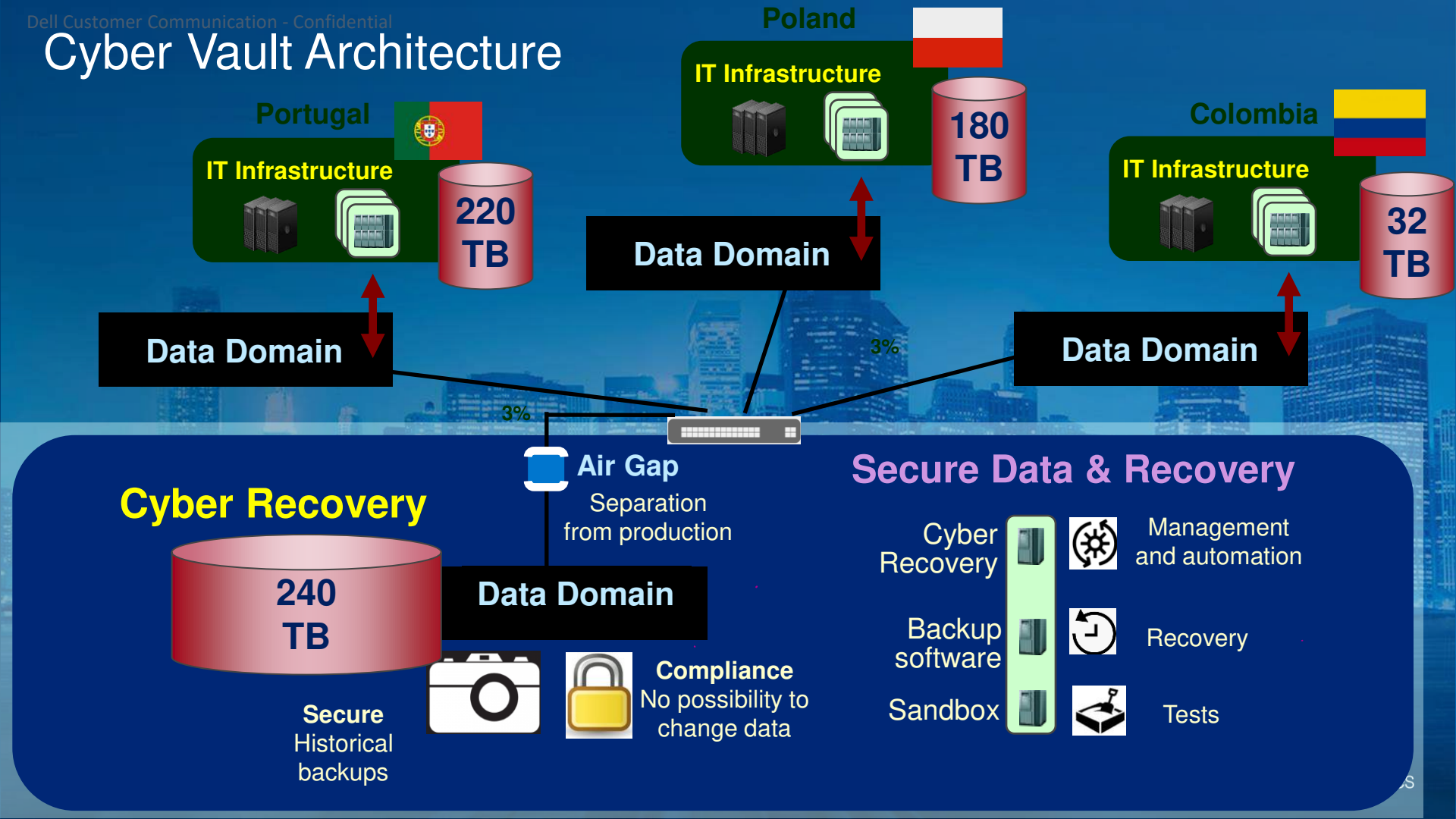
3. W przypadku ataku - zminimalizowanie czasu odtworzenia

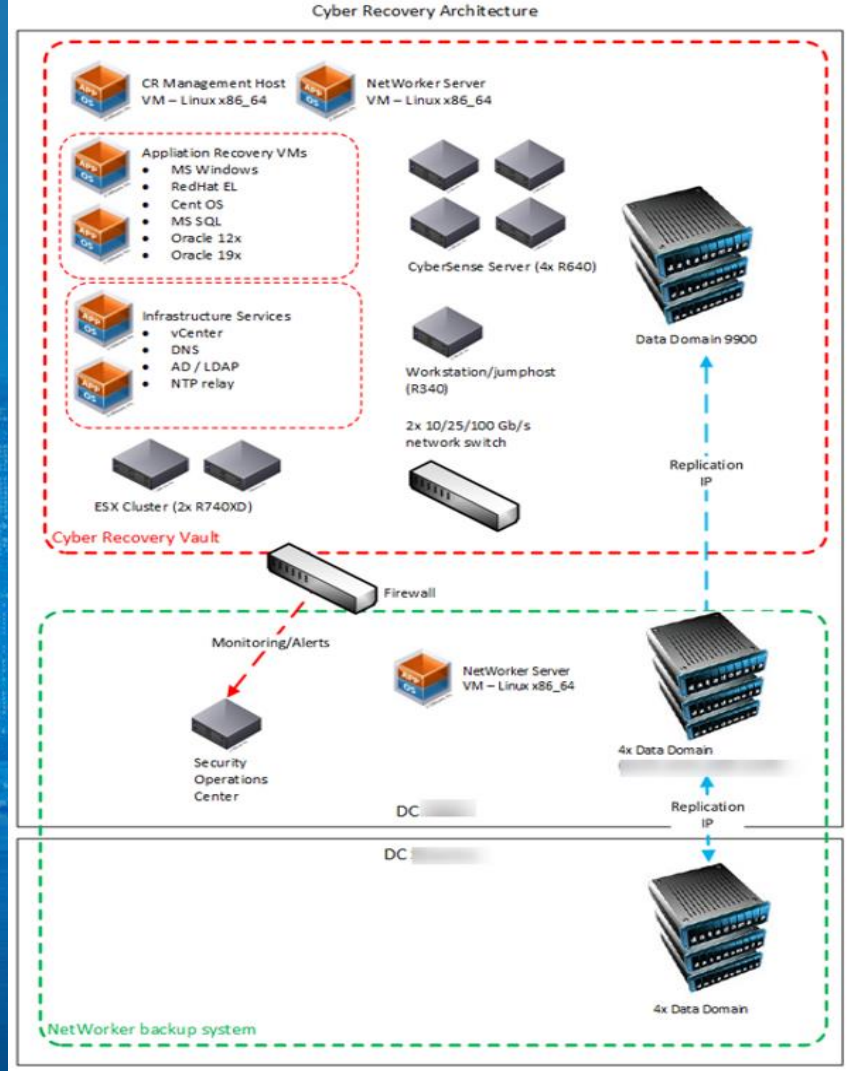
- Stworzenie Centrum testowo-odtworzeniowe
- Cykliczne odtworzenia krytycznych systemów
- Opracowane i przetestowane procedury odtworzeniowe
- Mozliwość testowania procedur

DELL Technologies

Dell Customer Communication - Confidential

Cyber Vault Architecture

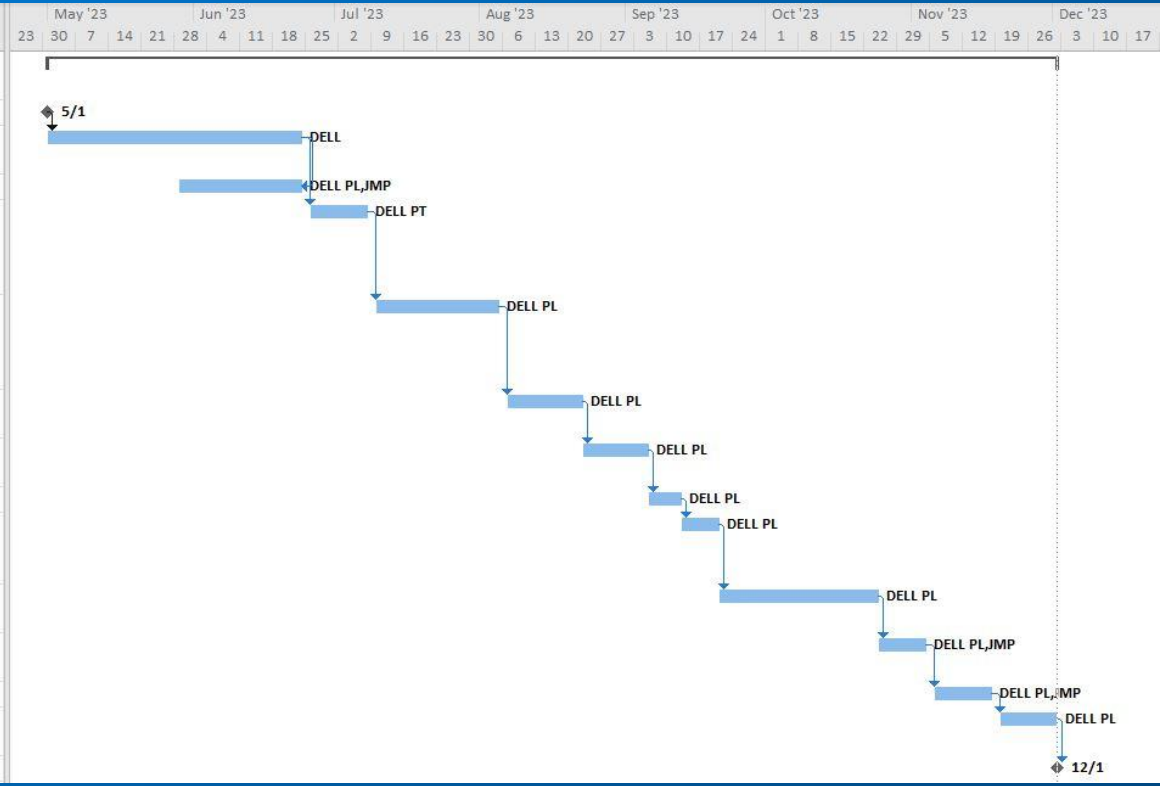




DELL Technologies

Przykładowy harmonogram wdrożenia

WBS	Task Name	Duration	Start	Finish	Resource Names
1	**Cyber Recovery - draft deployment plan**	**155 days**	**Mon 5/1/23**	**Fri 12/1/23**	
1.1	Order placed	0 days	Mon 5/1/23	Mon 5/1/23	JMP
1.2	Hardware production and delivery (estimate)	40 days	Mon 5/1/23	Fri 6/23/23	DELL
1.3	Cyber recovery design	20 days	Mon 5/29/23	Fri 6/23/23	DELL PL,JMP
1.4	Installation and configuration of hardware CE Vault infrastructure (DataDomain, servers, switches, KVM, firewall...)	10 days	Mon 6/26/23	Fri 7/7/23	DELL PT
1.5	Installation and configuration CR Vault software infrastructure (vSphere, Cyber Recovery, other elements)	20 days	Mon 7/10/23	Fri 8/4/23	DELL PL
1.6	Internal tests, optimisation, tunning	12 days	Mon 8/7/23	Tue 8/22/23	DELL PL
1.7	Installation, configuration and integration of CyberSense software	10 days	Wed 8/23/23	Tue 9/5/23	DELL PL
1.8	CS internal tests and optimisation	5 days	Wed 9/6/23	Tue 9/12/23	DELL PL
1.9	Preparing DR procedure for NetWorker server (1 NetWorker server)	6 days	Wed 9/13/23	Wed 9/20/23	DELL PL
1.10	Recovery procedures up to 3 systems	24 days	Thu 9/21/23	Tue 10/24/23	DELL PL
1.11	Disaster recovery tests for NetWorker server	8 days	Wed 10/25/23	Fri 11/3/23	DELL PL,JMP
1.12	Recovery procedures tests	10 days	Mon 11/6/23	Fri 11/17/23	DELL PL,JMP
1.13	Technical documentation preparation	10 days	Mon 11/20/23	Fri 12/1/23	DELL PL
1.14	Project finished	0 days	Fri 12/1/23	Fri 12/1/23	



© Copyright 2020 Dell Inc.

Zacznijmy już dziś!

Rekomendacje

Authentication, Identity & Security

- Active Directory / LDAP
- DNS dumps
- Certificates
- Event logs (including SIEM data)

Intellectual Property

- Source code
- Proprietary algorithms
- Developer libraries

Networking

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / microcode / patches

Host and Build Tools

- Physical/Virtual Platform Builds
- Dev Ops tools & automation scripts
- Firmware / microcode / patches
- Vendor software
  - Binaries (golden images)
  - Configurations & settings

Storage

- Backup hardware configuration
- SAN / array configurations
- Storage abstraction settings
- Firmware / microcode / patches

Documentation

- CMDB / asset D/R and Cyber Recovery Run-books &checklists
- Management extracts
- HR resources & contacts lists

© Copyright 2020 Dell Inc.

1. Jak przygotowujecie się do implementacji NIS 2?

2. Strategia Disaster Recovery to w zasadzie standard w każdej firmie a jak wygląda u Was strategia CR – Cyber Recovery?

3. Czy istnieje u Was plan odtworzenia po ataku cyfrowym na kluczowe dane ?

4. Jak realizowana jest separacja sieciowa oraz fizyczna dla trzeciej złotej kopii bezpieczeństwa? Czy jest zdalny dostęp do tych danych?

5. W jaki sposób kluczowe dane zabezpieczone są przed edycją, skasowaniem, zaszyfrowaniem (podatnościami na Ransoware, insider, hacker)

6. W jaki sposób weryfikujesz czy dane w backupie nie są zaszyfrowane?

7. W jaki sposób ustalisz, które dane należy odtworzyć, gdy środowisko produkcyjne lub jego cześć zostanie zaszyfrowane?

8. W jaki sposób chronisz platformę na której pracuje system do tworzenia kopii zapasowych tak, aby ona nie zostałą skompromitowana?

Cyfrowy Bunkier

Ochrona przed ransomware/hacker

Izolacja

Fizyczna i logiczna separacja danych

Niezmienność

Blokada przed edycją lub skasowaniem danych.

Gwarancja niezmienności danych

Weryfikacja

Analityka i wykrywanie ataków

Procedury

Przetestowane metody odtworzenia danych

© Copyright 2020 Dell Inc.


DELL Technologies