

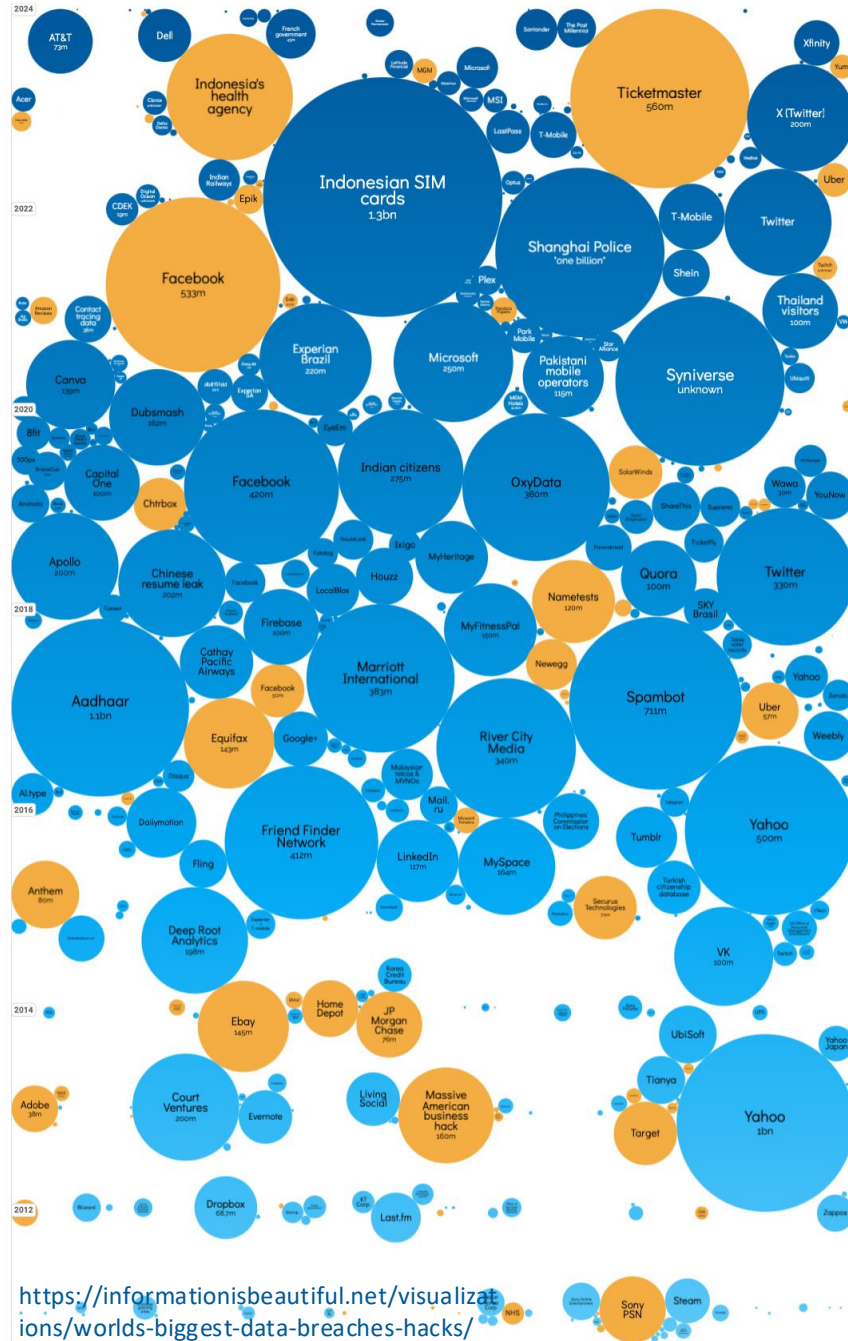
Zkušenosti s přípravou na nový ZoKB/NIS2, příklady z praxe od O2

Martin Dolný

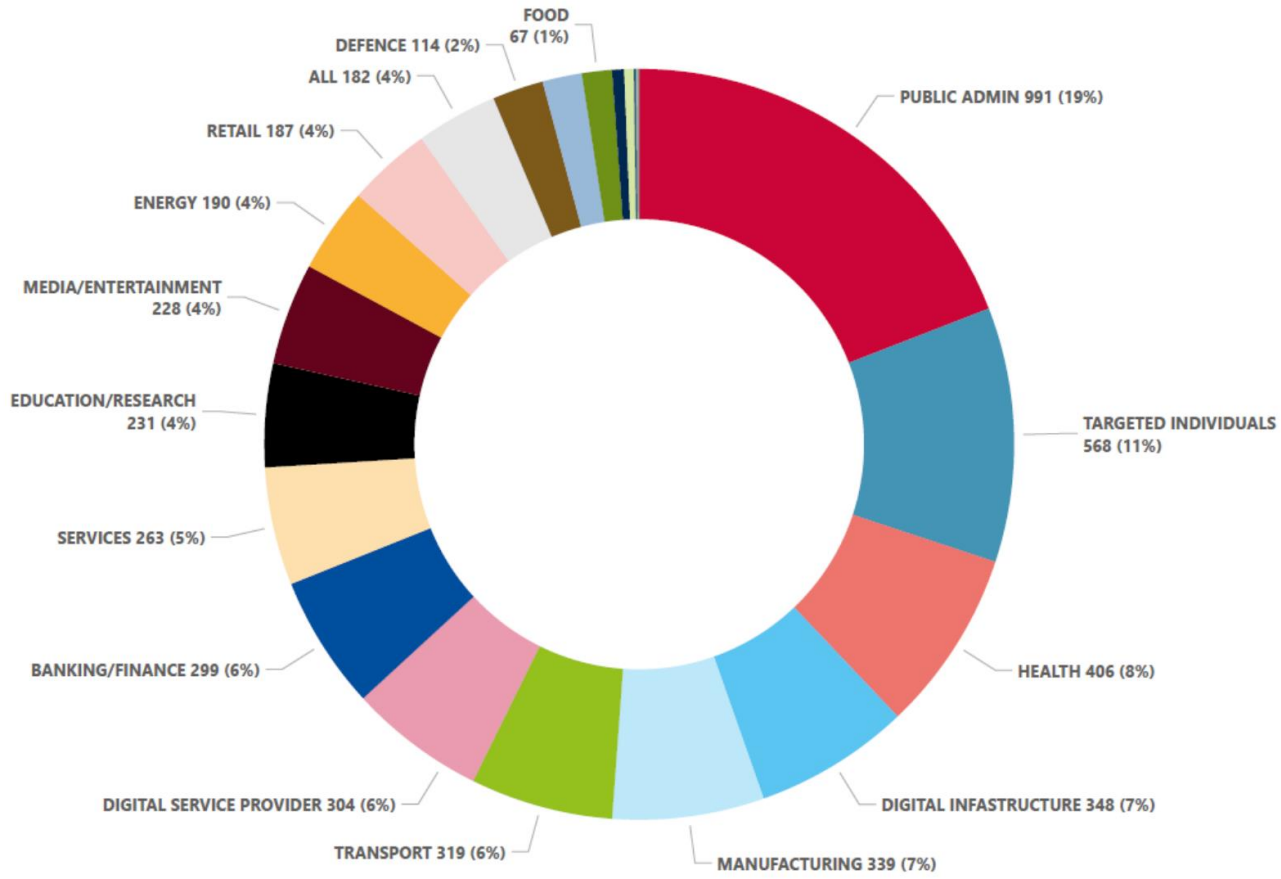
BDM, státní a veřejná správa

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records stolen



Nejčastější oběť KB útoků je státní správa



Počet KB útoků v ČR roste



Ministerstvo spravedlnosti ČR

@SpravedlnostCZ · [Sledovat](#)

Ministerstvo spravedlnosti od dopoledních hodin čelí kybernetickému útoku, který zasáhl provoz celého resortu, tedy [@SpravedlnostCZ](#), soudů, státních zastupitelství, [@ProbackaCz](#), [@vezenskasluzba](#) a rejstříku trestů. Dochází k postupnému obnovení provozu, za případné námi... [Zobrazit více](#)

2:35 odp. · 22. 10. 2024

5 Odpovědět Odkaz

[Další informace na platformě X](#)

Získejte všechny články jen za 690 Kč/rok

iDNES.cz

ZPRÁVY > KRAJE > KARLOVY VARY

[Zprávy](#) [Sport](#) [Okresy](#) [Tipy na výlet](#) [Jízdní řády MHD](#) [Galerie kreativců & Auta](#) [Náš kraj](#)

Radnici v Ostrově paralyzoval kybernetický útok, hackeři chtějí výkupné

12. září 2024 9:34



S následky rozsáhlého kybernetického útoku, který zásadně paralyzoval chod úřadu, se potýká radnice v Ostrově na Karlovarsku. Ten je obcí s rozšířenou působností a druhým největším městem karlovarského okresu. Systémy úřadu útoku čelily v noci na úterý. Podle místostarosty Jiřího Netrha útočníci data úřadu zašifrovali a za jejich odblokování požadují výkupné.

Získejte všechny články jen za 690 Kč/rok

iDNES.cz

ZPRÁVY > KRAJE > HRADEC KRÁLOVÉ

[Zprávy](#) [Sport](#) [Okresy](#) [Tipy na výlet](#) [Jízdní řády MHD](#) [Úspěchy východočeských firem](#) [Mistři oborů](#)

Hackeři napadli web úřadu na Rychnovsku a požadovali výkupné, šetří to policie

10. října 2024 17:55



Městský úřad dvoutisícového Borohrádku na Rychnovsku čelí hackerskému útoku. Neznámý pachatel zašifroval ransomwarem, tedy takzvaným vyděračským virem, elektronická data počítačového serveru a podle policie požadoval výkupné. Kriminalisté se případem zabývají od středy. Úřad zatím funguje v omezeném režimu.

KROK 1

CO

Posouzení aktuálního stavu a identifikace slabých míst kybernetické bezpečnosti

KDY

TEĎ! 01/24 – 12/24

PROČ

- Přehled aktuálního stavu kybernetické bezpečnosti
- Návrhy zlepšení a plán organizačně-procesní optimalizace
- Prioritizace pro nápravná opatření
- Harmonogram implementace
- Podklad pro rozpočet na KB

KROK 2, 3, 4...

CO

Řešení organizačních opatření dle standardů kybernetické bezpečnosti

- Identifikace primárních a podpůrných aktiv kybernetické bezpečnosti
- Analýza rizik
- Bezpečnostní dokumentace
- Vzdělávání pro rozvoj bezpečnostního povědomí
- Strategie Business Continuity Management

KDY

Do účinnosti ZoKB 07/25 a v rámci tranzičního období

PROČ

Kompletní a komplexní soulad kybernetické bezpečnosti s organizačně-procesními požadavky ZoKB

KROK n+

CO

Řešení technických opatření dle standardů kybernetické bezpečnosti

KDY

Dlouho/Střednědobý horizont

PROČ

Kompletní a komplexní soulad kybernetické bezpečnosti s technickými požadavky ZoKB

Nejčastější zjištění aktuálního stavu řízení KB

- 1 Není stanoven rozsah řízení kybernetické bezpečnosti
- 2 Neexistuje identifikace a řízení aktiv
- 3 Neexistuje identifikace a řízení rizik
- 4 Chybí DR a BCP plány, strategie a politiky
- 5 Nejsou definovány procesy řízení incidentů a změn (nebo v nich není začleněna bezpečnost)
- 6 Vrcholové vedení není začleněno v procesu řízení bezpečnosti
- 7 Bezpečnost je kompletně řízena IT oddělením
- 8 Neprovádí se penetrační testy a skeny zranitelností, nedostatečné zálohování a segmentace sítě
- 9 Nedostatečná ochrana koncových zařízení



Zkušenosti s přípravou na nový ZoKB

O₂

Soulad s organizačně procesními požadavky

Bezpečnostní
role

Řízení
kontinuity

Řízení přístupů
identit

Bezpečnost
komunikačních
sítí

Logování a
vyhodnocování
událostí

Aplikační
bezpečnost

Další opatření

Bezpečnostní role

- Zapojení vedení organizace do řízení KB
- Školení vedení, zaměstnanců, dodavatelů
- Osoba odpovědná za kybernetickou bezpečnost
- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Garant aktiva – primární i podpůrná aktiva
- Auditor kybernetické bezpečnosti

ity

Řízení přístupů
identit

Bezpečnost
komunikačních
sítí

Logování a
vyhodnocování
událostí

Aplikační
bezpečnost

Další opatření

Bezpečnost
role

- Vazba na primární aktiva - pořadí obnovy primárních aktiv
- Určení odpovědnosti, pravomoci
- Zálohování, šifrování záloh
- BC plány (per služba)
- Testování plánů kontinuity činností
- Metodický postup řízení incidentů
- Hlášení incidentů (všech / s významným dopadem)
- Zpráva o kybernetickém incidentu

ení přístupů
ntit

Bezpečnost
komunikačních
sítí

Logování a
vyhodnocování
událostí

Aplikační
bezpečnost

Další opatření

Řízení přístupů identit

Bezpečnostní
role

Řízení
kontinuity

- Každý uživatel jedinečný identifikátor
- Nezapomenout na technické účty!
- Vícefaktorová autentizace jako cíl
- Klíče, certifikáty, hesla
- Centralizovaný nástroj pro řízení oprávnění
- Pravidelné přezkoumání

Činnost
nिकाčních

Logování a
vyhodnocování
událostí

Aplikační
bezpečnost

Další opatření

Bezpečnostní
role

Řízení
kontinuity

Řízení přístupu
identit

- Oddělení provozního a zálohovacího prostředí
- Evidence povolených komunikací
- Bezpečné síťové protokoly
- Vzdálené přístupy a vzdálená správa aktiv
- Kryptografie
- Firewally, NGFW, aplikační firewally

ovávání a
odnocování
lostí

Aplikační
bezpečnost

Další opatření

Logování a vyhodnocování událostí

Bezpečnostní
role

Řízení
kontinuity

Řízení přístupů
identit

Bezpečnost
komunikačn
sítí

- Ochrana před škodlivým kódem – antiviry, EDR včetně jejich aktualizace – vazba na aplikační bezpečnost
- Kontrola dat na perimetru – FW, NGFW
- Včasné varování osob o incidentu
- Centrální nástroj pro detekci – best practise – log management, SIEM, SOAR
- Uchování logů

Aplikační
bezpečnost

Další opatření

Bezpečnostní
role

Řízení
kontinuity

Řízení přístupů
identit

Bezpečnost
komunikačních
sítí

Logování a
vyhodnocování
událostí

- Patch management
- Evidence nepodporovaných systémů, omezení jejich komunikace, náhradní bezpečnostní opatření
- Skenování zranitelností relevantních aktiv – vychází z řízení aktiv analýzy rizik
- Penetrační testy před uvedením do provozu a významných změnách
- Penetrační testy jako celku max. do 5 let.

šší opatření

Další opatření

Bezpečnostní
role

Řízení
kontinuity

Řízení přístupů
identit

Bezpečnost
komunikačních
sítí

Logování a
vyhodnocování
událostí

Aplikační
bezpečnost

- Fyzická bezpečnost - zamezení neoprávněného přístupu
- Evidence vstupů, detekce narušení
- Best-practise (kamery, EZS, EPS, VSS (CCTV), čidla v RACKu)
- Kryptografické klíče a certifikáty
- Systém správy klíčů – certifikační autority
- Průmyslová aktiva - ochrana před zranitelnostmi



Děkuji za pozornost

O₂