void
One service.
Zero worries.

SOITRON

Jarná ITAPA 2024

Martin Lohnert
void Security Operations Center

Void
One service.
Zero worries.

2018

- 200GB MongoDB v AWS
- Bez autentifikácie
- 445M záznamov o klientoch/partneroch s OÚ

Void
One service.
Zero worries.

2017

- Zraniteľnosť v Apache Struts
  - Patch 7.3.
  - Exploit 10.3.
  - Prienik 12.5.
- Prihlasovacie údaje
- Exfiltrácia OÚ 150M ľudí
- Detekcia po 75 dňoch (SSL cert)

Void
One service.
Zero worries.

Nov – Jan 2024

- Password spraying
- Prienik do *“legacy non-production test tenant account”*
- Následne *”very small percentage of Microsoft corporate email accounts, including [..]senior leadership team [..]cybersecurity, legal, and other functions”*

Void
One service.
Zero worries.

Mar 2024

- Útočník používa exfiltrované informácie
- Informácie boli zdieľané (aj) s klientami emailom
- Zdrojové kódy a prístupy do interných systémov

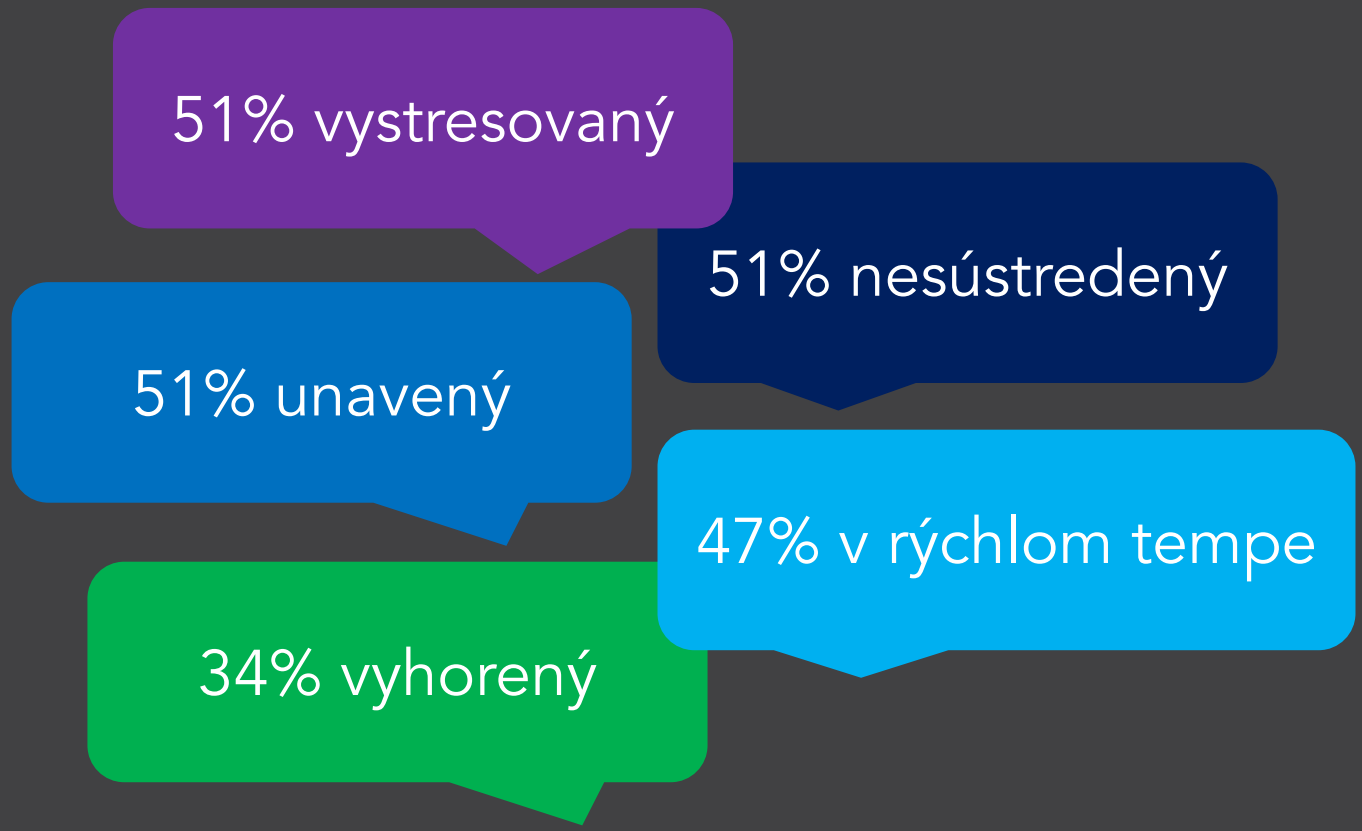
Void
One service.
Zero worries.

Ľudská chyba ako príčina incidentu

95% v IBM Cyber Security Intelligence Index
68% v Verizon Data Breach Investigations Report 2024
55% v Thales Data Threat Report 2023

Prečo ľudia robia chyby?

Nevedomosť
Zlé rozhodnutie
Prostredie



Tessian: The Psychology of Human Error 2022

Void
One service.
Zero worries.

Ako minimalizovať chyby?

Zmenšovať priestor pre omyl
Budovať povedomie a kultúru
Zlepšovať firemné prostredie
+ ?

Void
One service.
Zero worries.

SOITRON

Ďakujem za pozornosť

Martin LOHNERT
martin.lohnert@voidsoc.com
www.linkedin.com/in/martinlohnert
VOID Security Operation Center
www.voidsoc.com