Nicolai Brignoli

Founder & CEO ITNB AG

Automatisierte Bedrohungserkennung und Reaktion in der Praxis

11. Oktober 2023
it-sa, Nürnberg

itnb ag

IBM

Cost of a Data Breach Report - Gesundheitswesen

USD 10.9M

Durchschnittliche Kosten eines “Data Breaches” in der Gesundheitsbranche

Höchste Kosten im Vergleich zu den anderen Branchen

84% höher als der globale Durchschnitt von 4.45M

Globale Highlights

Top 3 initiale Angriffsvektoren

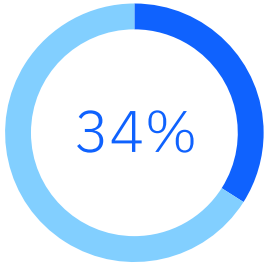
USD 5M

Durchschnittliche Kosten für Ransomware-bedingter Data Breach

USD 1.5M

Durchschnittliche Kostenersparung durch Incident Response (IR) Teams und Testing verglichen mit keinen IR Teams oder Testing

KI & Automatisierung

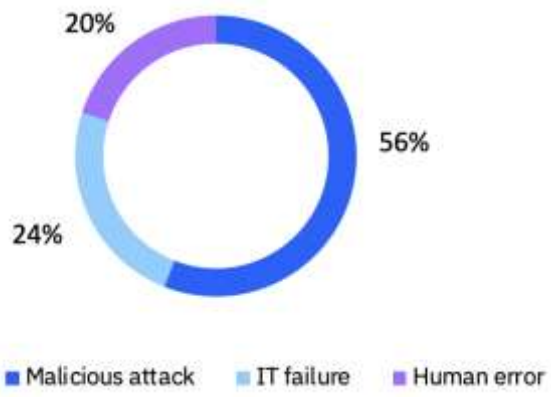


Prozent der Unternehmen im Gesundheitswesen nutzen bereits Security KI und Automatisierung

USD 850,000

Ersparnisse durch Securit AI und Automatisierung im Vergleich zu den durchschnittlichen Kosten eines Data Breaches weltweit

Ursachen für einen Data Breach



Zeit zur Identifizierung und Eindämmung

itnb ag

Reaktion in der Praxis

- **Die Schwachstelle ist meistens und weiterhin?**

  → Der Endpunkt!

  → Oder ist es der Mensch, die Technik, oder Phishing?

- **Die Lösung? Verhaltensanalyse und Reaktion!**

  → EDR mit SOCaaS! 24/7

itnb ag

Customer Experience

Healthcare sector, more than 5’000 licenses and 350 applications

Endpoint cases Detected and Remediated via IBM QRadar EDR & ITNB SOCaaS 24/7

1. Case 1 → Compromised Supplier (NDA) – Saturday 03:30 AM
   Tools used: among others, Nessus

2. Case 2 → Spear Phishing Mail (NDA) - Friday Evening 06:30 PM
   Revival of QakBot (QakNote) Email – Compromised Husband (IT Company)

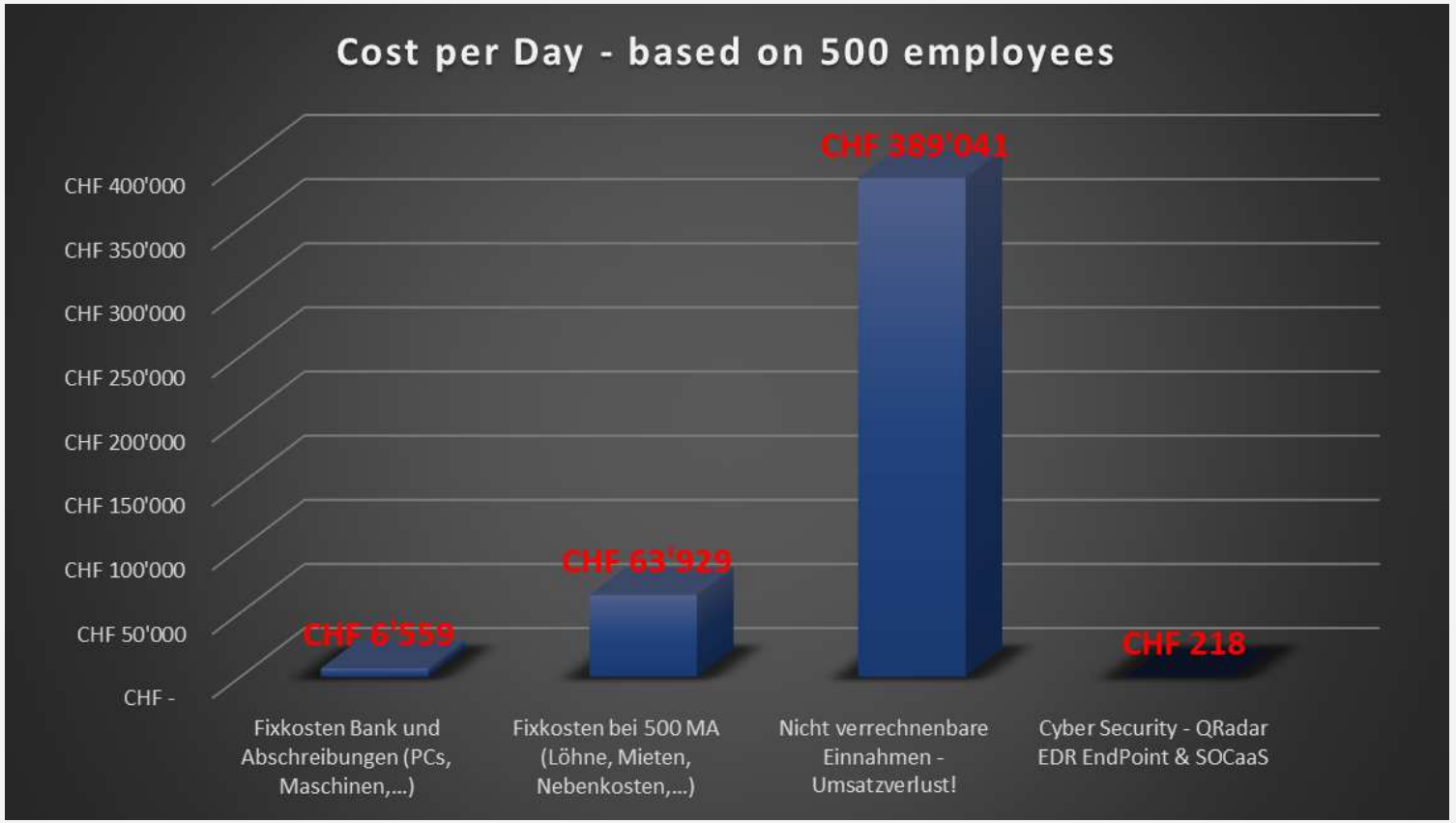
3. Case 3 → Brute Forcing - Password force (NDA)
   Attacker trying to guess a password by attempting several different passwords, every 30min 3 times (discovered by QRadar EDR Proactive Hunt Analysis Tool)

“The best gateway solution is of little help if the employee clicks, downloads or views something that is not secure. But what is secure? ***That's why we secure at least the endpoint!”***

itnb ag

Zusammenfassend

1. Durch **EDR *mit* SOCaaS 24/7** (MDR) **Effizienz optimieren** & **Wirksamkeit steigern**!
2. **Kosten reduzieren** denn: Bereits mit einer kleineren Investition, wird viel erreicht!



itnb ag

Mehr zu EDR & ASM?

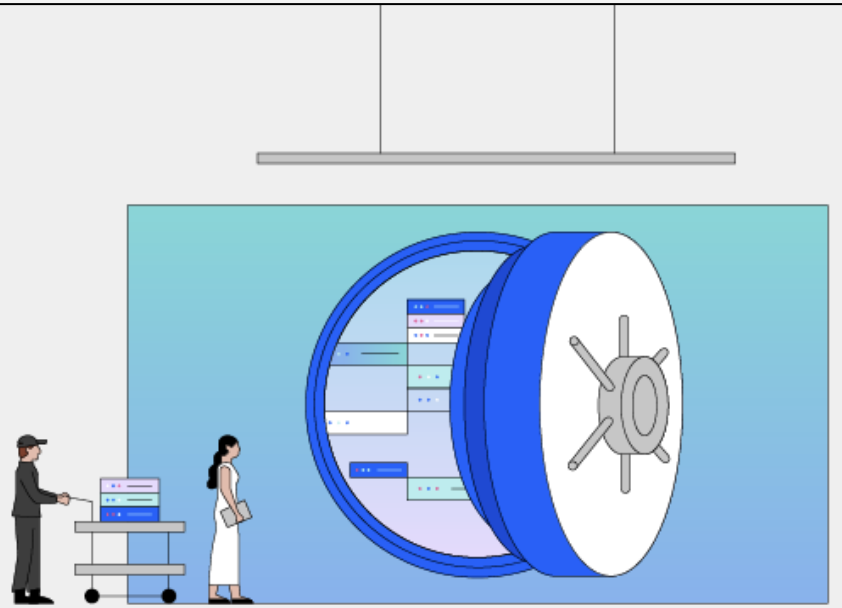
IBM **Security**

7A – 510

Visit us!

it-sa 2023 · 10. – 12. Oktober

Messe Nürnberg



IBM

itnb ag

«We preventively, predictively, and proactively help clients manage and secure their IT infrastructure!»

Head Office:

Suurstoffi 37, CH-6343 **Rotkreuz – ZG (Switzerland)**

Contact DACH:

Nicolai Brignoli

+41 79 620 75 41 (Mobile)

nicolai.brignoli@itnb.ch