IT-Security

Was braucht es wirklich und was ist Mythos?

Candid Wüest
Threat Researcher
@MyLaocoon

Data Breaches
383 Mio Marriott
Datensätze betroffen

SPAM/SCAM Emails
CEO Fraud kostet Milliarden
Emotet & Co lieben Makros

BYOD & Mobile
Unkontrollierte Geräte

Cloud & Shadow IT
Fehlkonfiguriert AWS S3,
Dropbox, GitHub,…

Ransomware
Travelex offline für 1 Monat
$6 Mio Lösegeld verlangt

Exponierte Services
RDP, Citrix, Pulse VPN,…

Supply Chain Attacken
ASUS verteilt Malware

Authentifizierung
Passwort Leak, Brute Force,…

Denial of Service (DoS)
Webseiten Ausfall

Regulationen
British Airways erhält
$230 Mio GDPR Busse

Wichtiger Grundschutz

1. **Sichere Email Konten**
   Multi Faktor, Konfiguration,…
2. **Starke Authentifizierung**
   Multi Faktor, Notify, OneTime,…
3. **Patch-Management**
   Software aktualisieren, Inventar,…
4. **Funktionierende Backups**
   Aktuell, schreibgeschützt,…
5. **Exponierte Services schützen**
   RDP evaluieren, Jump Host, Netzaufteilung,…
6. **Faktor Mensch**
   Mitarbeiter wissen wo Vorfälle melden

Kämpfen Sie nicht gegen APTs, solange Sie nicht vor Skript Kiddies geschützt sind!

Zusätzliche erweiterte/externe Optionen

PowerShell überwachen, Pentests, keine lokalen Admins,…

Sharon mccutcheon (Unsplash)


taringa.net
SCHAUEN SIE AM
RICHTIGEN ORT !
funny-picturess.us
ViralHog

Herzlichen Dank!

Candid Wüest
candid_wueest@symantec.com

Podcast: https://www.symantec.com/podcasts
Blog: https://www.symantec.com/blogs/threat-intelligence
ISTR: https://go.Symantec.com/istr