ADVANCED LAST LINE OF DEFENSE

Ihre Lebensversicherung gegen Totalverlust des Unternehmens
durch hochprofessionelle, staatlich verordnete Cyberbangriff(e)

Bulletin Juli 2022

cyberbreeze

Veränderte Bedrohungslage in 2022

- Angriffe verlagern sich zunehmend in den Cyberspace und sind Teil der neuen Kriegsführung
- Die militärische Auseinandersetzung in Europe erfordert umgehend zusätzliche Abwehrmaßnahmen
- Aufgrund der Sanktionen sind massive Gegenschläge durch die russische Cyberelite gestartet
- Diese Angreifer fokussieren heute ausschließlich auf die Vernichtung von Banken, Staat, kritischen Infrastrukturen, Verwaltung, Verteidigung etc.
- Das Vorgehen wird skrupellos bis hin zur Bestechung, Erpressung, Gewalt gegen interne Security-Stakeholder

Fazit: **Es geht aktuell um das Überleben Ihres Unternehmens!**

Angriffszenario #1: Command & Control.

- Ziel ist es, direkt und ohne Umweg die Security-Kernsysteme zu übernehmen
- Die übliche Perimeter Defense (Firewalls, Virenscanner usw.) werden insbesondere durch gezielte **Insider Attacs** einfach umgangen
- Im Fokus aktuell stehen EDR-Tools, IAM-Systeme – insbesondere Active Directory (AD) – sowie Softwareverteilungslösungen
- Der Reaktionszeiten minimieren sich bei diesen Angriffen massiv, eigentlich sogar gegen null

Fazit: **Es droht der totale Kontrollverlust quasi ad-hoc!**

Prominente Beispiele:

- Angreifer verschaffen sich domain-administrativen Zugriff auf die Sony-Systeme

- Angreifer löschen fast alle Active Directorys bei Maersk

- Übernahme des EDR-Tools von Carbon Black bei Krauss-Maffei durch die Angreifer

Unser Schutzschirm.

- ✓ Einsatz von advanced tools (deception, AI-based UBEA u.v.m.)
- ✓ Zusätzliches Monitoring für fortgeschrittene Angriffe installieren
- ✓ Last-Line-of-Defence-Konzept mit vertraulichen Prozeduren im „inner circle“ des Topp-Managements
- ✓ Anonyme Überwachung der „Wächter“ implementieren
- ✓ Gezielte Abschaltung von Kernsystemen einrichten
- ✓ Notfallprozesse gegen Insider-Attacken etablieren

Unser Tipp: Diese Maßnahmen unbedingt “undercover“ umsetzen!

PACKAGE: ADVANCED LAST LINE OF DEFENCE

PAKETINHALT:

- Screening der relevanten-Systeme hinsichtlich potentieller Insider-/State-sponsored-Angriffsvektoren
- Erstellung eines individuellen und streng vertraulichen LLD-Konzeptes
- Implementierung des neuen LLD-Konzeptes
- Herzstück bildet eine separierten Authentifizierung mit dem patentiertem Forced Forcing©-Schutz
- Lizenznutzungsgebühr Forced Forcing©
- Strike-Back-Procedures

Warum Cyberbreeze?

- Unsere Erfahrung aus aktiven Implementierungen
- Wir gehen einen Schritt weiter als die gängigen Anbieter + Konzepte
- Systemrelevante (DAX)-Unternehmen zählen zu unseren Kunden & Referenzen
- Beste Kontakte zu den global führenden Advanced Tool-Herstellern, Dienstleistern sowie RED-Teams
- Eigenes Patent für unschlagbar sichere, wissensbasierende Authentifizierungen
- Unserem Team besteht aus Ex-Vorständen global agierender Tier-1-Unternehmen
- Thomas Wolf zählt zu den wohl erfahrensten & intelligentesten Experten (Mitglied in der Giga-Society)

Fazit: **Klein, aber extrem fein und einzigartig!**

ADVANCED LAST LINE OF DEFENCE

Cyberbreeze
Platanenweg 2
63303 Dreieich
info@cyberbreeze.io

Mobile: +49-172-5614200
Sven Herrmann