base it

WIR STARTEN IN KÜRZE

WIR FREUEN UNS, DASS SIE DABEI SIND

BASE-IT PENTESTING: GEPLANTE CYBERANGRIFFE FÜR IHRE SICHERHEIT

PATRICK PONGRATZ

Consultant

2024-04-26

professional.
fast.
secure.

BASE-IT PENTESTING

Geplante Cyberangriffe für Ihre Sicherheit

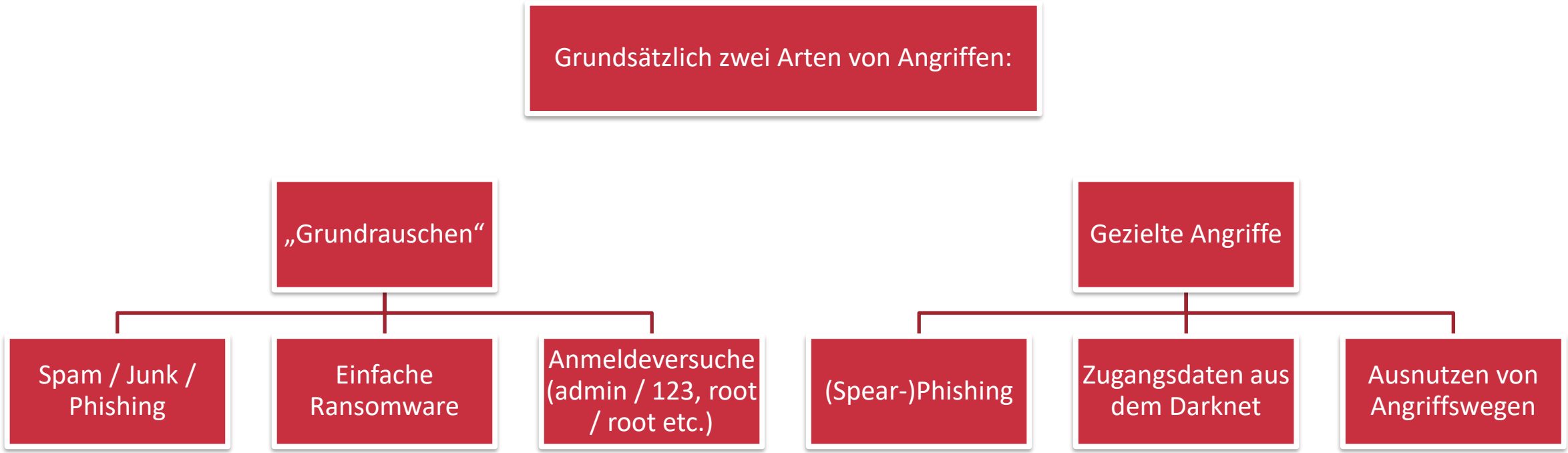
AGENDA

- Die Cyber-Bedrohungslage
- Was ist base-IT Pentesting
  - Ziele
  - Vorgehensweise
  - Der Bericht
- Einfügung in die Gesamtsicherheit

BEDROHUNGEN

DIE CYBER-BEDROHUNGSLAGE

Geplante Cyberangriffe für Ihre Sicherheit



GEZIELTE ANGRIFFE

Geplante Cyberangriffe für Ihre Sicherheit

Ransomware: Durchschnittlich ~10 Tage im Netzwerk

Erweiterte Angriffe: mehrere Monate

Längste Zeit: Informationsgewinnung – „mithören“

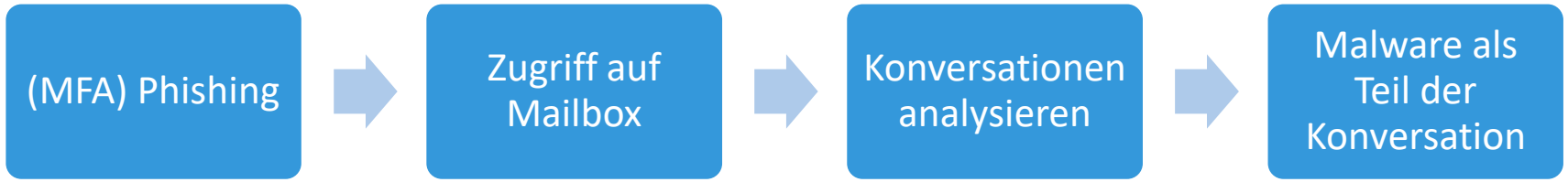
Dieser Angriff wird simuliert – im Schnellverfahren

PHISHING

Geplante Cyberangriffe für Ihre Sicherheit

ANGRIFFE ZIELGERICHTETER

- Business Email Compromise



EXPLOITATION

Geplante Cyberangriffe für Ihre Sicherheit

EXPONIERTE SYSTEME

- Business-Lösungen häufig als primäres Ziel (high risk / high reward)
  - CVE-2023-48788: Fortinet FortiClient EMS SQL Injection (Leading to RCE -> MSSQL)
  - CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect
- Schwachstellen vor Veröffentlichung in Telegram-Kanälen gehandelt

STOLEN CREDENTIALS

Geplante Cyberangriffe für Ihre Sicherheit

DARKNET-MARKETPLACES

- Passwortwiederverwendung
- Passwörter aus anderen Angriffen

BRUTEFORCE / PASSWORD-SPRAYING

- Auf Endpunkte ohne Absicherung dagegen
- Wiederverwendung der Passwörter auf sensibleren Endpunkten

GEZIELTE ANGRIFFE - EINTRITTSPUNKTE

Geplante Cyberangriffe für Ihre Sicherheit

base it

1

Phishing

Client-Workstation

2

Exploitation

(DMZ) Server

Fremdes Netzwerkgerät

3

Stolen Credentials

VPN

GEZIELTE ANGRIFFE - AUSWIRKUNGEN

Geplante Cyberangriffe für Ihre Sicherheit

- Zwei Hauptgründe
  - Geld verdienen / Erpressung (Ransomware Gruppierungen)
  - Wirtschaftsspionage (State-Actors)
- So viel Zugriff wie möglich
  - Mailbox Vorstand
  - Finanztransaktionen
  - Research & Development
  - Backups
  - Domain-Admin / Global-Admin / Cluster-Admin

base it

PENTESTING

WAS IST EIN PENETRATION TEST

Geplante Cyberangriffe für Ihre Sicherheit

„Ein Penetration Test ist eine systematische Überprüfung der Sicherheit eines Computersystems oder Netzwerks.

Es simuliert einen Angriff eines potenziellen Hackers, um Schwachstellen und Sicherheitslücken zu identifizieren.

Ziel ist es – unter anderem –, die Systeme und Prozesse eines Unternehmens zu verbessern und sicherzustellen, dass wichtige Daten und Ressourcen vor unerwünschtem Zugriff und Manipulation geschützt sind.“

BASE-IT PENTESTING ANSATZ

Geplante Cyberangriffe für Ihre Sicherheit

- Standardisiert…
  - Wir halten uns an anerkannte Vorgehensweisen
  - Wir kategorisieren und bewerten Schwachstellen nach definierten Standards
  - Wir verwenden Tools & Techniken, die auch in echten Angriffen vorkommen
- …aber mehr als Standard!
  - Weit mehr als ein Vulnerability Scan
  - Erfahrung im Bereich SOC, Incident Handling, Operating von Microsoft Umgebungen und Security Consulting
  - Nur durch Erfahrung & Kreativität können Angriffe erfolgreich simuliert werden

ZIELE

Geplante Cyberangriffe für Ihre Sicherheit

- Überblick über das aktuelle Gesamtsicherheitsniveau
- Aufdecken von relevanten Schwachstellen
- Testen bestehender Abwehrmechanismen
- Erstellung eines umfänglichen Berichts
  - Zusammenfassung der Überprüfung
  - Bewertung des Risikos und Auswirkungen gefundener Schwachstellen
  - Direkte Empfehlungen zum Schließen von Sicherheitslücken
  - Mittel- bis langfristige Roadmap zur Erhöhung der Sicherheit
- Baseline zur externen und internen Überwachung

VORGEHENSWEISE

Geplante Cyberangriffe für Ihre Sicherheit

- Interner Penetration Test
  - Simulation eines Angriffs:
    - Ausgehend von einer Client Workstation
    - Über ein fremdes Netzwerkgerät
    - Durch Kompromittierung eines VPN / Terminalserverzugangs
    - Weitere Szenarien möglich
  - Keine Simulation der initialen Kompromittierung
    - Kein Phishing / Social Engineering
  - Evaluierung realistischer Angriffspfade

VORGEHENSWEISE

Geplante Cyberangriffe für Ihre Sicherheit

- Externer Penetration Test
  - Simulation eines Angriffs:
    - Über das Internet
  - Informationsgewinnung aus öffentlichen Quellen (OSINT)
  - Überprüfung von extern erreichbaren
    - VPN-Logins
    - Webseiten
    - Management-Oberflächen
  - Keine (D)DoS-Angriffe

VORGEHENSWEISE

Geplante Cyberangriffe für Ihre Sicherheit

- Web Application Penetration Test
  - Simulation eines Angriffs:
    - Auf eine bestimmte Applikation
  - Test auf Schwachstellen (OWASP)
  - Überprüfung der Berechtigungsstruktur
  - Fuzzing von Input
  - Idealerweise Test-Umgebung
  - Source-Code Audit

VORGEHENSWEISE

Geplante Cyberangriffe für Ihre Sicherheit

WHITE BOX

Wir analysieren Ihre IT-Systemumgebung auf Konfigurationsfehler, Sicherheitslücken und identifizieren Verbesserungspotentiale

mit vollem Zugriff auf Quellcode und Dokumentation

VORTEIL

maximale Schwachstellenerkennung

NACHTEIL

irrelevante Schwachstellen
hoher Zeitaufwand
unrealistische Hackerperspektive

GREY BOX

Wir nehmen einen gezielten, realitätsnahen Angriffsversuch vor mit dem Ziel der Kompromittierung von sensiblen Unternehmensdaten, Benutzerkonten und IT Systemen

mit Informationen zu Infrastrukturdokumentation & Systemumgebung

VORTEIL

realistische Schwachstellen
minimale Bereitstellung von Dokumentation / Zugang

NACHTEIL

weniger Schwachstellen

BLACK BOX

Wir nehmen einen realitätsnahen Angriffsversuch vor mit dem Ziel der Kompromittierung von sensiblen Unternehmensdaten, Benutzerkonten und IT Systemen

Zero Access zu Infrastrukturdokumentation, Systemumgebung, Quellcodes und andere Dokumentationen

VORTEIL

realistischste Schwachstellen
geringer Vorbereitungsaufwand

NACHTEIL

unvollständige Schwachstellen wegen zeitintensiver Informationsgewinnung

BEISPIEL: INTERNER GREY-BOX PENTEST

Geplante Cyberangriffe für Ihre Sicherheit

- Zur Verfügung gestellte Informationen / Zugänge
  - Überblick VLAN-Segmente
  - Liste von besonders sensiblen Konten / Gruppen
  - Grober Überblick über eingesetzte Technologien
  - Client-Workstation mit niedrig privilegiertem Userkonto
  - Netzwerkzugriff: 1x mit aktivierter NAC, 1x ohne aktivierte NAC

BEISPIEL: INTERNER GREY-BOX PENTEST

Geplante Cyberangriffe für Ihre Sicherheit

- Durchgeführte Tätigkeiten (Auszug)
  - Allgemeine Umgebungsanalyse (Active Directory, Softwareverteilung, Berechtigungsmanagement)
  - Schwachstellenscans
  - Überprüfung der Clientsicherheit (Berechtigungserhöhung, Persistence, AV/XDR Detection)
  - Angriffe auf Netzwerkprotokolle (Spoofing)
  - Durchsuchen der Freigaben und Wissensdatenbanken auf sensible Informationen
  - Checken auf Standardpasswörter

BASE-IT PENTESTING

Vorbereitung

1 Definition der Testmethodik

White-Box / Grey-Box / Black-Box

2 Definition des Scopes & Rahmenbedingungen

Auswahl der Ziele, Ausnahmen, Umgang mit kritischen Findings

3 Technische Ansprechpartner

Benachrichtigung bei Findings, wer ist bei Problemen erreichbar, wer stellt Zugang / Hardware bereit

4 Bereitstellung notwendiger Ressourcen

Besprechungsräume, VPN-Zugänge, User Accounts, Hardware (Clients, Peripherie, Testgeräte), Dokumentation (Netzwerkplan etc.)

5 Permission to Attack (+ NDA)

Formelle Berechtigung zum Testen der IT-Umgebund

BASE-IT PENTESTING

Ablauf (technisch)

1

Informationsgewinnung

Erhebung von Informationen über Ziele im Scope

Portscanning, OSINT, Dokumentation

2

Schwachstellenanalyse

Automatische Überprüfung auf bekannte Schwachstellen

Vulnerability Scanner, Web-Scanning, Fuzzing

3

Manuelle Überprüfungen

Ausnutzung von Schwachstellen und Simulation von Angriffen

PoCs anpassen, Impact evaluieren, priorisieren von realistischen Angriffen

DER BERICHT

Geplante Cyberangriffe für Ihre Sicherheit

- Überblick über den Auftrag
- Management Summary
  - Wie steht es um die Gesamtsicherheit
  - Welche Schwachstellen waren besonders kritisch
  - Wie sollte die Sicherheit verbessert werden
- Zusammenfassung aller Schwachstellen
  - Kategorisiert und kontextuell bewertet
  - Nachvollziehbarkeit & Wiederholbarkeit gewährleisten
  - Beschreibung von Impact, Risiko und empfohlenen Gegenmaßnahmen
- Roadmap
  - Langfristige Strategie zur Erhöhung der Sicherheit

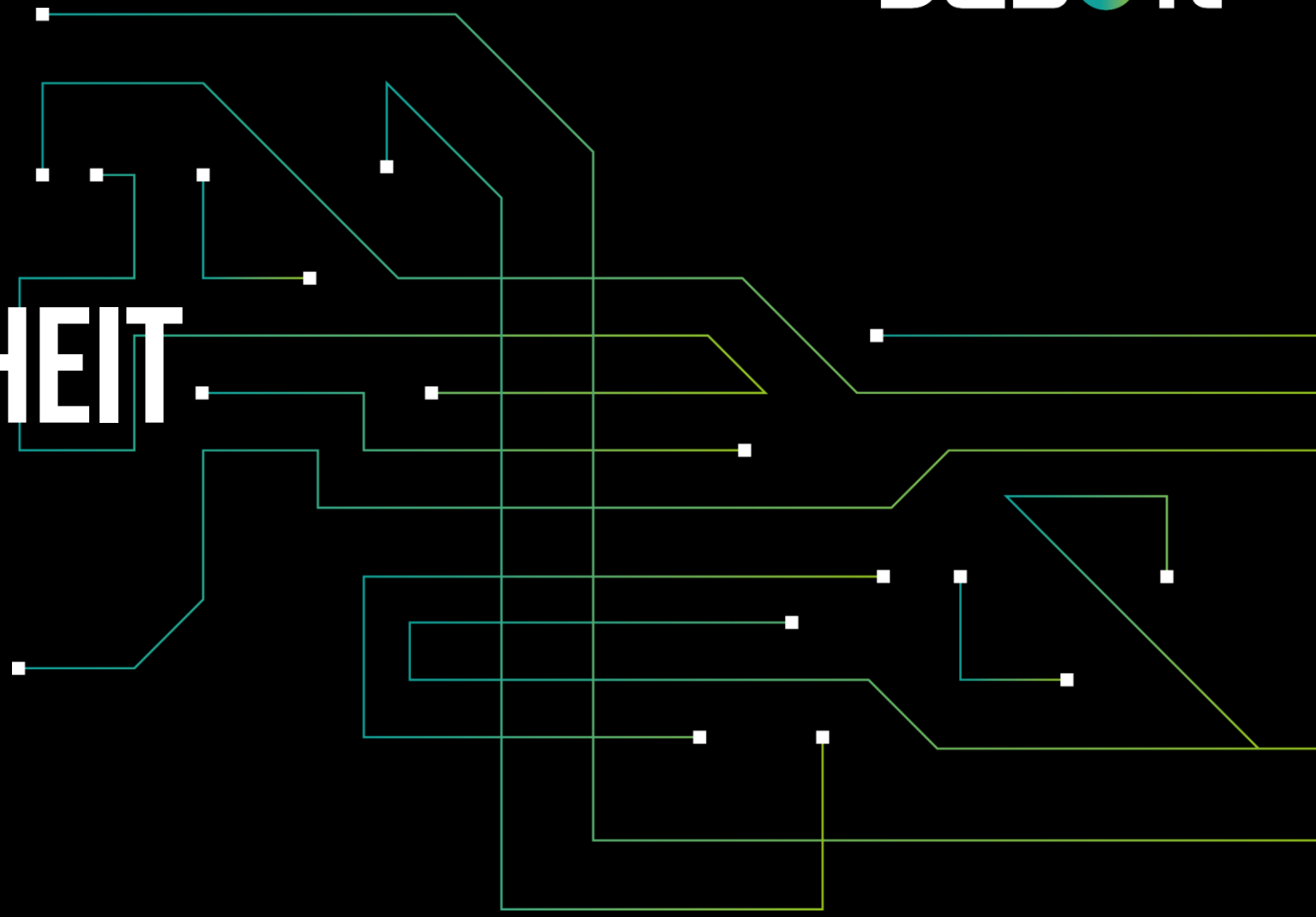
ROADMAP

Geplante Cyberangriffe für Ihre Sicherheit

- Kurzfristige Maßnahmen
  - Sind in den einzelnen Schwachstellenkapitel enthalten
  - Helfen gegen akute Probleme
- Langfristige Maßnahmen
  - Bedürfen Planung
  - Müssen priorisiert werden
  - Erhöhen die Sicherheit nachhaltig
  - Roadmap beinhaltet unsere Expertise, welche priorisiert werden sollten

base it

GESAMTSICHERHEIT



GESAMTSICHERHEIT

Geplante Cyberangriffe für Ihre Sicherheit

- Pentest zeigt konkrete, ausnutzbare Probleme auf
  - kontextuell bewertet mit Auswirkungen
- Wichtige Basis zur Priorisierung von Gegenmaßnahmen
  - Welche Systeme / Endpunkte sind besonders exponiert?
  - Werden Angriffe erkannt?
  - Greifen Hardening Maßnahmen wie gewünscht?
  - AV / EDR / WAF Lösungen Stand der Technik?
- Kontinuierliche Entwicklung des Sicherheitsniveaus (im Scope!)
- Schulung und Awareness der IT-Teams und Management

Thank you!

base it

Ansfelden | Salzburg | Vienna

+43 7229 87800 - 0 | office@baseit.at | www.baseit.at

our digital company broschure