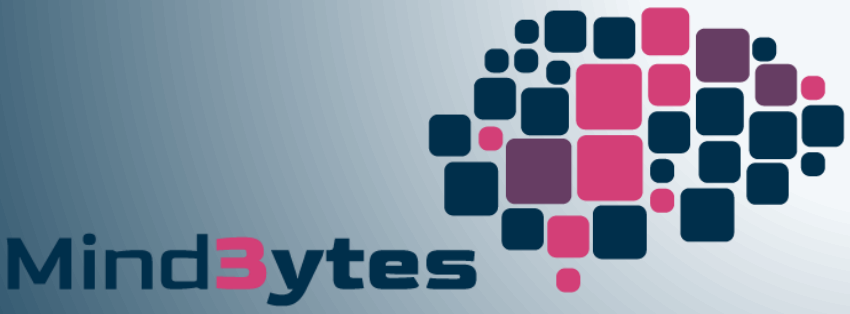


Pentesting & Red Teaming

Planung, Tipps, Erzählungen

MindBytes in Kooperation mit Oberberg-Online Informationssysteme

Überblick nächste 30 Minuten

1. **Kurze Vorstellung**
   Damit ihr wisst, wer hier spricht.
2. **Pentests**
   Klärung der W-Fragen.
3. **Pentests**
   Planung & Ablauf.
4. **Red Teaming**
   Vergleich & Abgrenzung zu Pentests.
5. **Einblicke in Projekte**
   Aus dem Nähkästchen.
6. **Q&A**
   Open End

MindBytes – Wer wird sind

3 Gründer & Geschäftsführer
Jeweils 6-8 Jahre Erfahrung in der IT-Sicherheitsbranche

Gegründet 2023

Spezialisiert auf das Aufdecken von Schwachstellen und Angriffssimulationen (Pentesting & Red Teaming)

Christian Stehle
Stuttgart
(OSCP, CRTO, OSEP, OSWE, CRTP, ...)

Nina Wagner
Freiburg
(OSCP, CRTO, CARTP)

Simon Holl
Hamburg
(OSCP, OSEP, BSCP)

Pentest: Was ist das?

Kurz für „Penetrationstest“. Hat nichts mit Stiften zu tun.

Pentest – Was ist das (nicht)?

- ✓ Aufdecken von technischen Schwachstellen
- ✓ Mensch involviert
- ✓ Prüfung der Wirksamkeit von Maßnahmen
- ✓ Zielgerichtet + risikoorientiert

- ✗ Reiner Schwachstellen-Scan
- ✗ Lasttest / Denial-Of-Service
- ✗ Social Engineering / Phishing
- ✗ Kontinuierlich im Sinne von 24/7

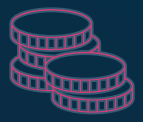
Aufgepasst: „Pentest“ ist kein feststehender Begriff

Pentests: Warum & Wann?

5 Gründe für Pentests

- Risiko erfolgreicher Angriffe reduzieren
  (Umsatzverlust, Datenlecks, Reputationsschäden, ...)
- Vertrauen von Kunden und Partnern stärken
- Regulatorische Vorgaben, wie NIS2
- Kosten sparen bei Cyber-Versicherungen
- Sicherheit frühzeitig mitdenken, um später davon zu profitieren




Ausgangssituationen & Ansätze

Typische Ausgangs-situationen

Wir wissen nicht, wo wir stehen

NIS2 kommt

Wir wissen nicht, wie wir priorisieren sollen

Wir wissen nicht, ob unsere Maßnahmen wirksam sind

Ansatz über Pentesting & Red Teaming

- Einnehmen der Perspektive von Angreifern, um realitätsnah Risiken aufzudecken
- Einbeziehen von IT, Menschen, Prozessen & physischen Maßnahmen
- Beantwortung der Frage: „Was könnte unter welchen Umständen passieren?“
- Empfehlung zur priorisierten Planung von Maßnahmen

Was ist wann geeignet?

	PENTESTING		REDTEAMING
Ist-Zustand zu IT-Sicherheit	Neues Thema / Unklare Situation	Erste Maßnahmen umgesetzt	Umfangreiche Maßnahmen umgesetzt
	Konzept-Gespräch zur Abstimmung des gemeinsamen Vorgehens		
Projekt-Beispiele	• Pentest von außen • Phishing zur Awareness-Messung • Pentest von innen	• Erweiterter Pentest von innen • Wichtige Web-anwendungen • Gezielte Tests zur Angriffserkennung	• Angriffssimulation • Physische Sicherheit • Social Engineering

Pentest: Wann & wann nicht?

- ✔ Bestandsaufnahme
- ✔ Begleitend bei der Entwicklung
- ✔ Nach Änderungen
- ✔ Regelmäßige Tests zu neuen Angriffstechniken

- ✘ Zeitnahe Ablösung geplant
- ✘ System unwichtig (Priorisierung passt nicht)
- ✘ Änderungen innerhalb des Testzeitraums geplant

Pentests: Planung & Ablauf

Übersicht Planung & Ablauf

1

Interne Planung

Aktuellen Stand erfassen und sinnvolle Pentests planen.

2

Konzept-Gespräch

Gemeinsames Ausarbeiten eines passenden Konzepts.

3

Vorbereitung

Zeitliche und organisatorische Abstimmung für eine reibungslose Zusammenarbeit.

4

Durchführung

Aufdecken und Dokumentieren von Schwachstellen.

5

Nachbereitung

Auslieferung des Berichts und Abschlussbesprechung.

6

Retest / Weiterführende Pentests

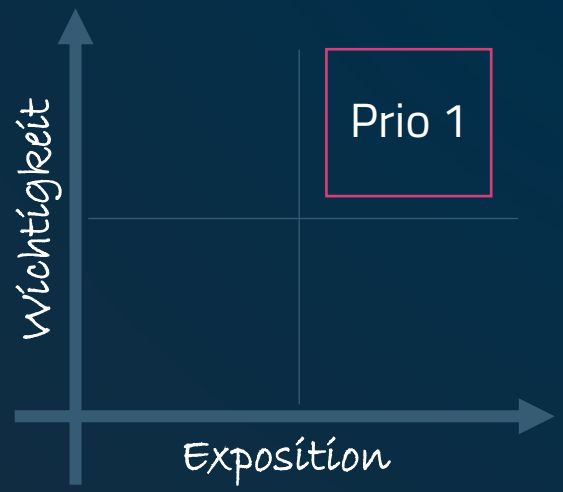
Interne Planung

Wichtige Unternehmenswerte klarmachen

Relevante Systeme identifizieren

Angriffsoberfläche / Exposition der Systeme bewerten

Priorisieren von Systemen & Anwendungen



Ablauf Pentest

Vorher

- Ansprech-person
- Worst-Case / Schwerpunkte
- Zeitraum für Durchführung
- Zugriff regeln

Durchführung

- Info bei Start & Ende
- Aktueller Kenntnisstand
- Manuelle Tests
- Sofort-Meldung bei kritischen Schwachstellen
- Erprobte Tools

Nachher

- Abschluss-besprechung
- Ergebnis-bericht

Ergebnisbericht

- Vollständiger Beispielbericht zum Download auf Webseite www.mind-bytes.de

Ergebnisbericht: Management Summary

1 Management Summary

Testgegenstand: Interne Firmeninfrastruktur

Anzahl der Findings: 7, dabei kann ein Finding mehrere Assets betreffen.

Gesamtrisiko

- Die Findings ermöglichen eine einfache Ausbreitung im internen Netzwerk, die aufgrund von fehlenden Erkennungsmechanismen mutmaßlich auch nicht bemerkt werden würde. Der erste Schritt ins interne Firmennetz sollte stets als realistisch betrachtet werden, z. B. durch Phishing oder physischen Zugriff vor Ort.
- Mögliche Folgen eines erfolgreichen Angriffs sind das Stilllegen der IT und Produktion durch Ransomware sowie die Veröffentlichung von firmeninternen Daten im Internet.
- Dabei entstehende Kosten können über folgende Faktoren abgeschätzt werden: 1) Personal- und Beratungskosten beim Reagieren auf einen Angriff, 2) Umsatzverlust durch einen Betriebsausfall, 3) Wiederherstellungskosten, z. B. für die Neueinrichtung von Systemen, 4) Rufschaden, 5) Strafen durch Vertragsverletzungen, z. B. wenn Fristen nicht eingehalten werden können, 6) Compliance-Verstöße, z. B. gegen branchenspezifische Regelungen oder Datenschutzverletzungen.

Handlungsbedarf: Dringend

Gesamtrisiko im Vergleich zu anderen Unternehmen[1]**:** Durchschnittlich

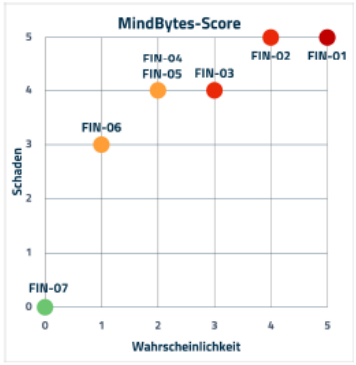


Abbildung 1 - Verteilung nach Schaden und Wahrscheinlichkeit

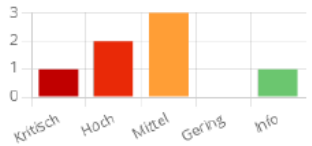


Abbildung 2 - Verteilung nach Gesamtrisiko

[1] Dies ist eine relative Einschätzung und lässt keine Rückschlüsse über die Gefährdungslage zu.

Ergebnisbericht: Übersicht Handlungsempfehlung

1.1 Handlungsempfehlung

Die Einschätzung zur Behebung basiert auf unserer Erfahrung und sollte intern validiert werden. In der Regel resultieren erfolgreiche Angriffe aus der Verkettung von mehreren Schwachstellen, weshalb wir eine Behebung aller Findings empfehlen.

Maßnahmen	Behebung	Hinweise zur Behebung	Findings
Quick Wins ⚡	⌚ Dringend ⌛ Stunden 💰 Nein	Die Findings können voraussichtlich mit geringem Aufwand behoben werden und bringen ein relevantes Sicherheitsplus.	3.2 FIN-02: Rechteerweiterung durch verwundbare Zertifikatsvorlage 3.5 FIN-05: Zugriff auf interne Infrastruktur aus Gäste-WLAN möglich 3.6 FIN-06: Inkonsistente Verwendung von LAPS
Konfiguration	⌚ Dringend ⌛ Tage 💰 Nein	Die interne Umgebung muss genauer analysiert werden, um ungewünschte Nebeneffekte zu vermeiden.	3.1 FIN-01: Verwendung von einfach erratbaren Passwörtern 3.4 FIN-04: Manipulation von LDAP-Kommunikation möglich
Neue Konzepte	⌚ Mittelfristig ⌛ Wochen 💰 vermutlich	Konzeptionelle Änderungen sind erforderlich, welche eine genaue Planungsphase benötigen. Die niedrige Bewertung von FIN-07 ist darauf zurückzuführen, dass dies keine technische Schwachstelle, sondern ein fehlender Angriffserkennungs-/Abwehrmechanismus ist.	3.3 FIN-03: Keine dedizierte Umgebung für administrative Tätigkeiten 3.7 FIN-07: Keine Erkennung von auffälligem Verhalten im Netzwerk

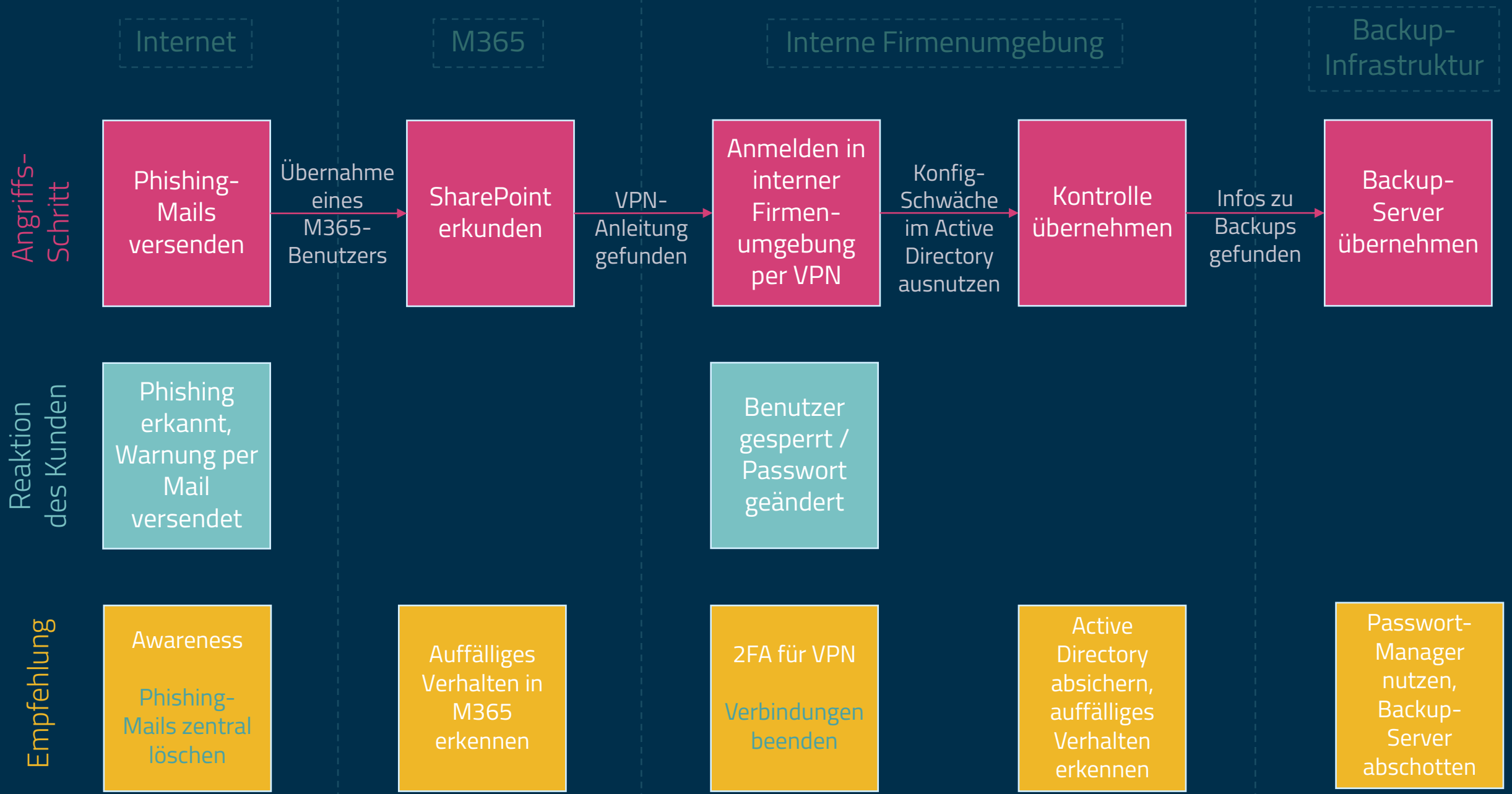
⌚ Priorität: dringend / mittelfristig / langfristig | ⌛ Geschätzte Behebungsdauer je Finding: Stunden / Tage / Wochen | 💰 Entstehen Kosten: nein / vermutlich (nicht) / ja

Und was ist eigentlich Red Teaming?

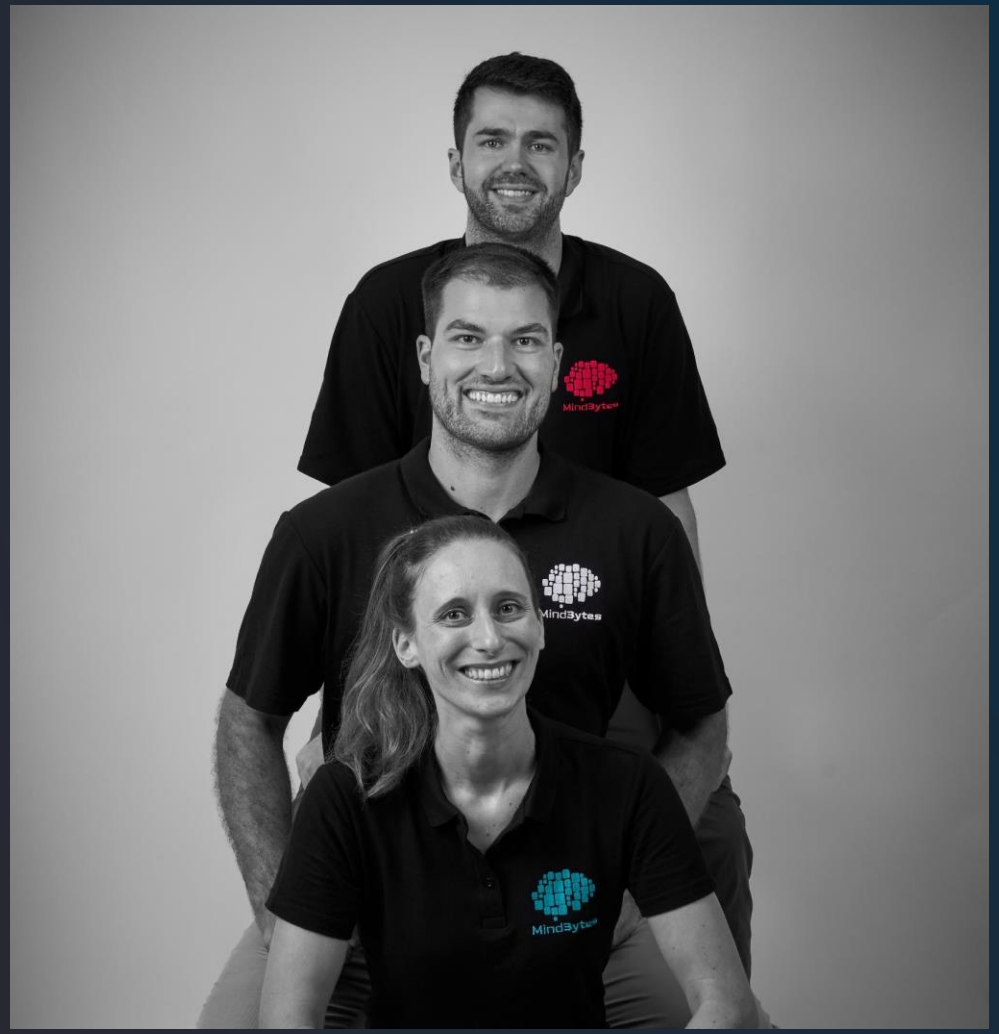
Vergleich

	Pentesting	Red Teaming
Ziel	Möglichst viele technische Schwachstellen durch manuelle & automatisierte Prüfungen aufdecken	Technische und organisatorische Schwachstellen im Unternehmen aufdecken, ggf. mit Social Engineering und ggf. auch physisch vor Ort; Realitätscheck zu Angriffserkennung und -abwehr
Testgegenstand	Ein festgelegter Testgegenstand, wie eine IT-Umgebung oder Webanwendung	Gesamtes Unternehmen/Organisation inkl. Reaktionsfähigkeiten auf Angriffe; Überprüfen von vereinbarten Szenarien, wie z. B. Kontrollübernahme über IT oder Backups
Kommunikation	Angekündigte Tests, alle relevanten Personen auf Kundenseite wissen Bescheid	So wenig wie möglich Personen auf Kundenseite wissen Bescheid, um Ergebnisse nicht zu verfälschen
Vorgehen	Möglichst tiefgehendes, effizientes Testen; Wir können “laut” sein, denn bspw. das Auslösen von Alarmen ist egal	Zielgerichtetes Vorgehen in Szenarien, wir agieren „leise“ und wollen (erstmal) nicht auffallen

Einblicke in Projekte


Internet
M365
Interne Firmenumgebung
Backup-Infrastruktur
Angriffs-Schritt
Phishing-Mails versenden
Übernahme eines M365-Benutzers
SharePoint erkunden
VPN-Anleitung gefunden
Anmelden in interner Firmen-umgebung per VPN
Konfig-Schwäche im Active Directory ausnutzen
Kontrolle übernehmen
Infos zu Backups gefunden
Backup-Server übernehmen
Reaktion des Kunden
Phishing erkannt, Warnung per Mail versendet
Benutzer gesperrt / Passwort geändert
Empfehlung
Awareness
Phishing-Mails zentral löschen
Auffälliges Verhalten in M365 erkennen
2FA für VPN
Verbindungen beenden
Active Directory absichern, auffälliges Verhalten erkennen
Passwort-Manager nutzen, Backup-Server abschotten

Fragen?



Kontakt

hallo@mind-bytes.de
+49 711 20709567
https://mind-bytes.de

MindBytes GmbH
Probststr. 15
70567 Stuttgart

Amtsgericht Stuttgart, HRB 790784
Ust-IdNr. DE363069855

vertreten durch die Geschäftsführung
Christian Stehle, Nina Wagner, Simon Holl