(PSST… DA WILL SICH JEMAND AN IHRER IT VERGREIFEN.)
WETTEN, DASS DIE DAS SCHAFFEN?

SIE DENKEN, IHR IT-SYSTEM IST SICHER?
WIR WETTEN DAGEGEN!

Das Prinzip ist ganz einfach: Sie lassen uns eine kostenlose, völlig ungefährliche Hacker-Simulation powered by Safebreach in vier Kategorien durchführen. Wenn wir erfolgreich sind, buchen Sie einen unserer Security-Workshops. Wenn nicht, gehen wir mit fünf Mitgliedern Ihres Teams niveauvoll essen – auf unsere Rechnung. **Na, wetten Sie mit?**

SIE GEWINNEN DIE WETTE …

… wenn bei unserer Hacker-Simulation in keiner der fünf getesteten Kategorien mehr als 50 % der Angriffsmethoden erfolgreich waren.

SIE BUCHEN EINEN WORKSHOP …

… wenn mindestens 50 % der Angriffsmethoden der Hacker-Simulation in einer Kategorie erfolgreich waren, etwa bei bekannten Angriffen.

POTENZIELLE SCHÄDEN BEI UNGESICHTERTER IT.

CYBERANGRIFFE FÜHREN ZU ENORMEN VERLUSTEN.

Hacker entziehen Werkzeug-Hersteller **sensible interne Daten** und drohen mit Veröffentlichung. IT-Systeme müssen heruntergefahren und neu aufgesetzt werden. Neben **finanziellen Schäden** auch **hoher Imageschaden**.

Schadsoftware Emotet durch E-Mails schaltet **Universität zwölf Tage offline**
Weitere Schadsoftware wird nachgeladen, mit der Hacker Daten klauen und zerstören..

IT-Systeme internationaler Juwelierkette lahm gelegt und Daten **verschlüsselt**. Juwelier zahlt **hohe Lösegeld** Forderung.

Schad-Datei greift Netzwerk führenden Beleuchtungsherstellers an. Festnetz und E-Mail Zugang nicht mehr erreichbar, es kommt zu **Produktionsausfällen**. IT-Infrastruktur muss **neu aufgesetzt** werden.

Trojaner durch E-Mails legt Elektro-Großhandel Möhle für **drei Wochen** lahm. Hohe Lösegeldsumme von rund **120.000 Euro** für Freikauf des Unternehmens.

Geschätzter Gesamtschaden
102,9 Mrd. € jährlich*

Hohe Dunkelziffer
Tatsächlicher Schaden im deutschen Mittelstand
heute nicht öffentlich sichtbar

Die größte Gefahr: Städte ohne Strom, gehackte Krankenhäuser
"Das Schlimmste ist, wenn kritische Infrastruktur von sowas betroffen wird. Die müssen wir schützen. Wir reden von Wasserwerken, Elektrizitätswerken; wenn ganze Städte und Landstriche plötzlich von der Energieversorgung abgeschnitten sind", **sagt Maurice Marrali, Kriminalkommissar vom Cyberdezernat Saarbrücken**

Alle Daten verschlüsselt
Man kann nur reagieren und hängt von Sachen ab, die man selbst nicht beeinflussen kann. Das ist eine ganz harte Geschichte.
Gerhard Klein, Opfer von Cyberkriminalität

Elektrokonzern wird um 21 Mio. Euro erpresst
Schadsoftware verschlüsselt Buchhaltungsdaten eines großen Elektrokonzerns. Zur Freigabe sollen ca. 21. Mio. Euro in Bitcoins gezahlt werden. Das Unternehmen macht keine Angaben, ob das Lösegeld gezahlt wurde.

ERLEBEN, WAS VERBINDET.

*bitkom (2019): Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr#item-5554-2-close

DIE WETTE IM DETAIL

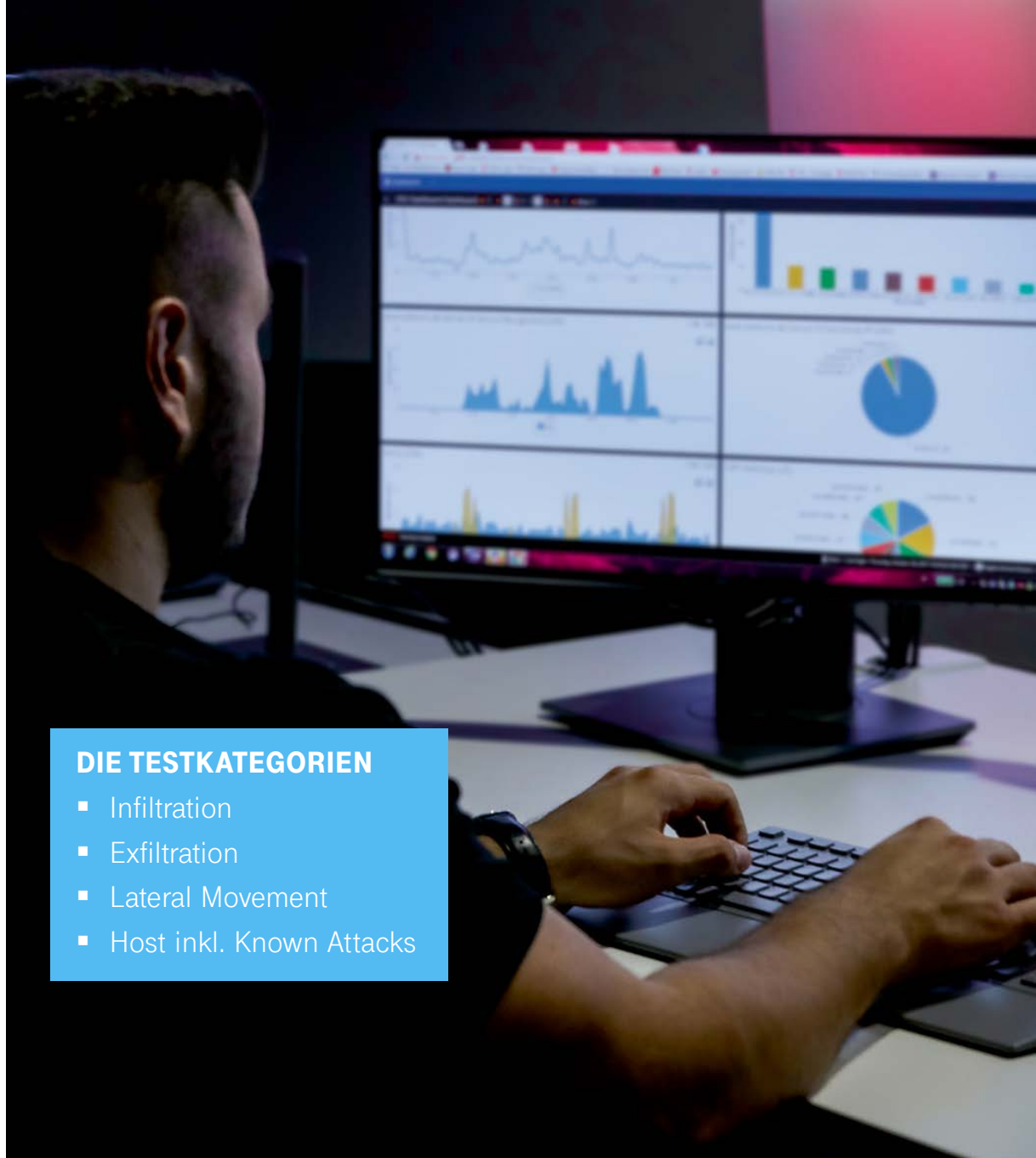
DAS SOLLTEN SIE WISSEN (1/3)

Die Safebreach Hacker-Simulation

- Die Hacker-Simulation kostet **normalerweise ca. 1.900 €**
- Im Rahmen dieser Wette ist der Test für Sie völlig kostenlos, aber garantiert nicht umsonst

So läuft die Wette

- Wir vereinbaren einen Informations-Call mit Ihnen
- Absprache des Testablaufs und der Voraussetzungen
- Wir installieren gemeinsam mit Ihnen 3–10 Simulatoren an ausgewählten Stellen
- Die Simulation dauert etwa einen Tag
- Anschließend: Auswertung, Ergebnis-Präsentation



DIE TESTKATEGORIEN

- Infiltration
- Exfiltration
- Lateral Movement
- Host inkl. Known Attacks

DIE WETTE IM DETAIL
DAS SOLLTEN SIE WISSEN (2/3)

Was müssen Sie tun?

- Sie nehmen am Informations-Call teil
- Sie beschreiben Ihre eingesetzten Sicherheitslösungen
- Gemeinsam wählen wir die Simulatoren-Standorte aus
- Sie geben uns die „Permission to attack“
- Installation der Messpunkte an den festgelegten Simulatoren-Standorten
- Einrichtung der Firewall Freigaben: Die Simulatoren müssen ausgehende Verbindungen über Port 80/443 aufbauen können

Was benötigen wir von Ihnen?

- Informationen über die Netzwerkarchitektur
- Client-Freigabe zur Server-Kommunikation über 80/443 zwischen Simulatoren und Safebreach Management
- Einen technischen Ansprechpartner
- Festlegung eines Zeitraums für die Wette

DIE WETTE IM DETAIL
DAS SOLLTEN SIE WISSEN (3/3)

Was wird getestet?

- Wir simulieren verschiedene Phasen eines Angriffs:
  - Infiltration
  - Lateral Movement
  - Exfiltration
  - Host inkl. der „Known-Attacks“
- Dabei werden verschiedene Angriffsmethoden zwischen den Simulatoren simuliert
- Je nach Simulator werden Host-, Netzwerk- oder nur Netzwerk-Angriffe simuliert
- Durch die Tests wird klar, ob eingesetzte Sicherheits-mechanismen wie Firewall, Anti-Virus, HTTP Proxy etc. zuverlässig funktionieren

Keine Gefahr für Ihr Netz!

- Unsere Tests finden nur zwischen den installierten Endpunkten statt: Gefahren sind ausgeschlossen
- Die Simulatoren sollten auf Referenz-Systemen installiert werden, um den Produktionsbetrieb nicht zu stören

Das Ergebnis

- Wir werten die Testresultate aus
- Sie erhalten Reports zu den Ergebnissen
- Die Ergebnisse werden im Rahmen einer Telefon-konferenz oder bei Ihnen vor Ort präsentiert

SIE GEWINNEN DIE WETTE?
GUTEN APPETIT!

Wir laden Sie zum Essen ein

- Wir laden Sie und weitere 4 Mitarbeiter/innen Ihres Teams in ein gemeinsam ausgewähltes Restaurant in Ihrer Nähe ein
- Ob IT-Leiter, Geschäftsführer, Security-Beauftragter oder Netzwerkspezialist: Sie entscheiden, wer dabei ist
- Von unserer Seite kommen der Vertriebsbeauftrage und/oder der Vertriebsleiter mit

ERLEBEN, WAS VERBINDET.

SIE VERLIEREN DIE WETTE?

WILLKOMMEN ZUM WORKSHOP!

Vier nachfolgende, individuelle Analyseworkshops bieten maßgeschneiderte Beratung, Betrachtung und konkrete Security-Tipps für Ihre spezifische IT-Landschaft.

In diesem Fall haben Sie zwar unsere kleine Wette verloren, gewinnen aber viel Zukunftssicherheit!

Alternativ haben Sie auch die Möglichkeit mit einem speziellen Industrie Security Check ihr Produktionsnetz auf Schwachstellen zu prüfen.

SCHWACHSTELLENANALYSE S

- Analyse Ihres Sicherheitsniveaus
- Identifikation von Sicherheitslücken mit Schwachstellenscannern
- Maßnahmendefinition, um die Sicherheitslücken zu schließen
- Herstellerneutrale Empfehlungen
- Ergebnispräsentation per WebEx: Länge: 2–3 h

1.095 €

PENETRATION TEST KOMPAKT M

- Orientiert am BSI-Durchführungskonzept (Bundesamt für Sicherheit in der Informationstechnik)
- Individuell auf Ihre Systeme abgestimmte Testschwerpunkte
- Umfangreiche Maßnahmendefinition, um die Sicherheitslücken zu schließen
- Ausführliche Dokumentation inklusive Risikobewertung und Maßnahmendefinition
- 2 Tage Test, Ergebnispräsentation vor Ort oder WebEx

3.895 €

PENETRATION TEST L

- Akkreditiertes Prüfschema
- Orientiert am BSI-Durchführungskonzept
- Individuell auf ihre Systeme abgestimmte Testschwerpunkte
- Umfangreiche Maßnahmendefinition, um die Sicherheitslücken zu schließen
- Ausführliche Dokumentation inklusive Risikobewertung und Maßnahmendefinition
- 4 Tage Test, Ergebnispräsentation vor Ort oder WebEx

5.995 €

INDUSTRIAL SECURITY CHECK

- Überprüfung der eingesetzten Geräte und Protokolle
- Detaillierter Maßnahmenkatalog mit Empfehlungen
- Individuell auf Ihre Systeme abgestimmte Testschwerpunkte
- Aufdecken von Sicherheitslücken in Produktionsnetzen
- Orientiert am Durchführungskonzept des BSI
- 2 Tage Test, Ergebnispräsentation vor Ort oder WebEx

4.595 €

Alle Preise zzgl. gesetzl. USt.

ERLEBEN, WAS VERBINDET.

VIELEN DANK