BreakinLabs

Penetrationstests:

Der Unterschied zwischen Unternehmenserfolg und einem unerwarteten Ende ...

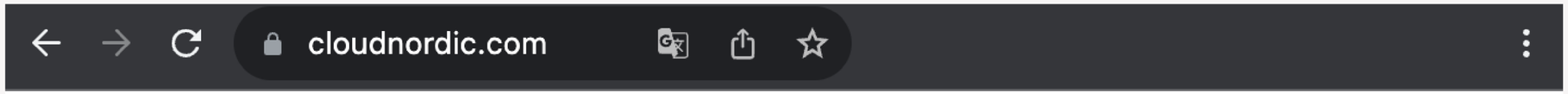
Who am i?

Thomas Moosmüller

M.Sc. Informatik
IT seit 16 Jahren
6 Jahre freiberuflicher IT-Security Consultant
4 Jahre als Geschäftsführer der BreakinLabs GmbH
Zertifizierungen: CISSP, OSCE, OSEP, OSCP, CEH

Das “Problem”

Der Morgen, an dem die Welt tausender Unternehmer stillstand



Für Kunden in CloudNordic

Leider wurde CloudNordic in der Nacht vom Freitag, den 18.08.2023 um 04:00 Uhr einem Ransomware-Angriff ausgesetzt, bei dem kriminelle Hacker alle Systeme lahmlegten. Websites, E-Mail-Systeme, Kundensysteme, Websites unserer Kunden usw. Alles. Ein Einbruch, der CloudNordic völlig lahmgelegt hat und der auch unsere Kunden hart trifft.

Da wir den finanziellen Lösegeldforderungen der kriminellen Hacker nicht nachkommen können und wollen, haben das IT-Team von CloudNordic und externe Experten intensiv daran gearbeitet, einen Überblick über den Schaden zu erhalten und zu ermitteln, was wiederhergestellt werden konnte.

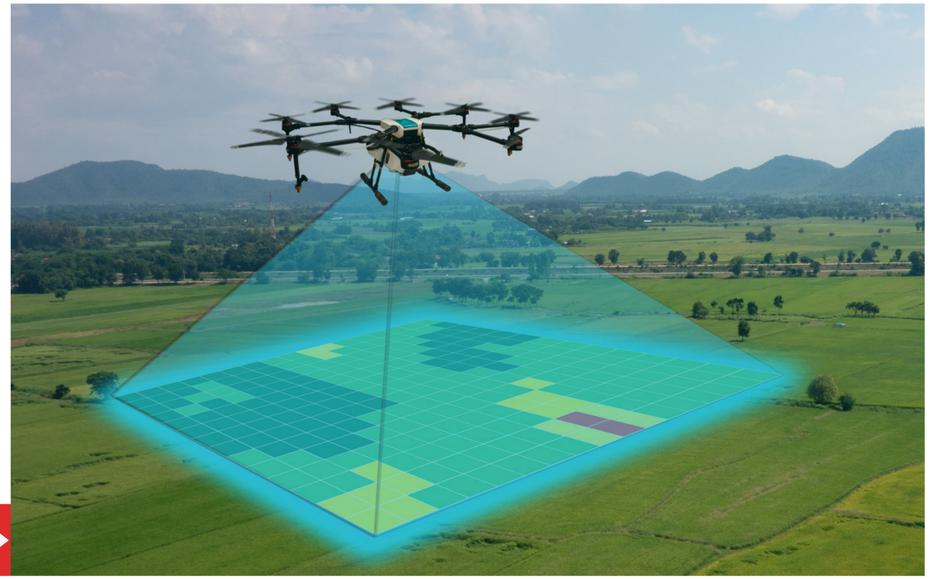
Leider war es nicht möglich, weitere Daten wiederherzustellen, und der Großteil unserer Kunden hat somit sämtliche Daten bei uns verloren. Dies gilt für alle, die wir zu diesem Zeitpunkt noch nicht kontaktiert haben.

Der Hackerangriff wurde der Polizei gemeldet.

Was sind Penetrationstests?

Der Unterschied zwischen "denken, sicher zu sein" und "wirklich sicher sein"

Vulnerability Scan



Penetrationstest

Ansätze bei Pentests

Blackbox-Pentest

- realitätsnah
- unvoreingenommen
- schneller Start

Whitebox-Pentest

- detailiert
- genauer
- kostenintensiver

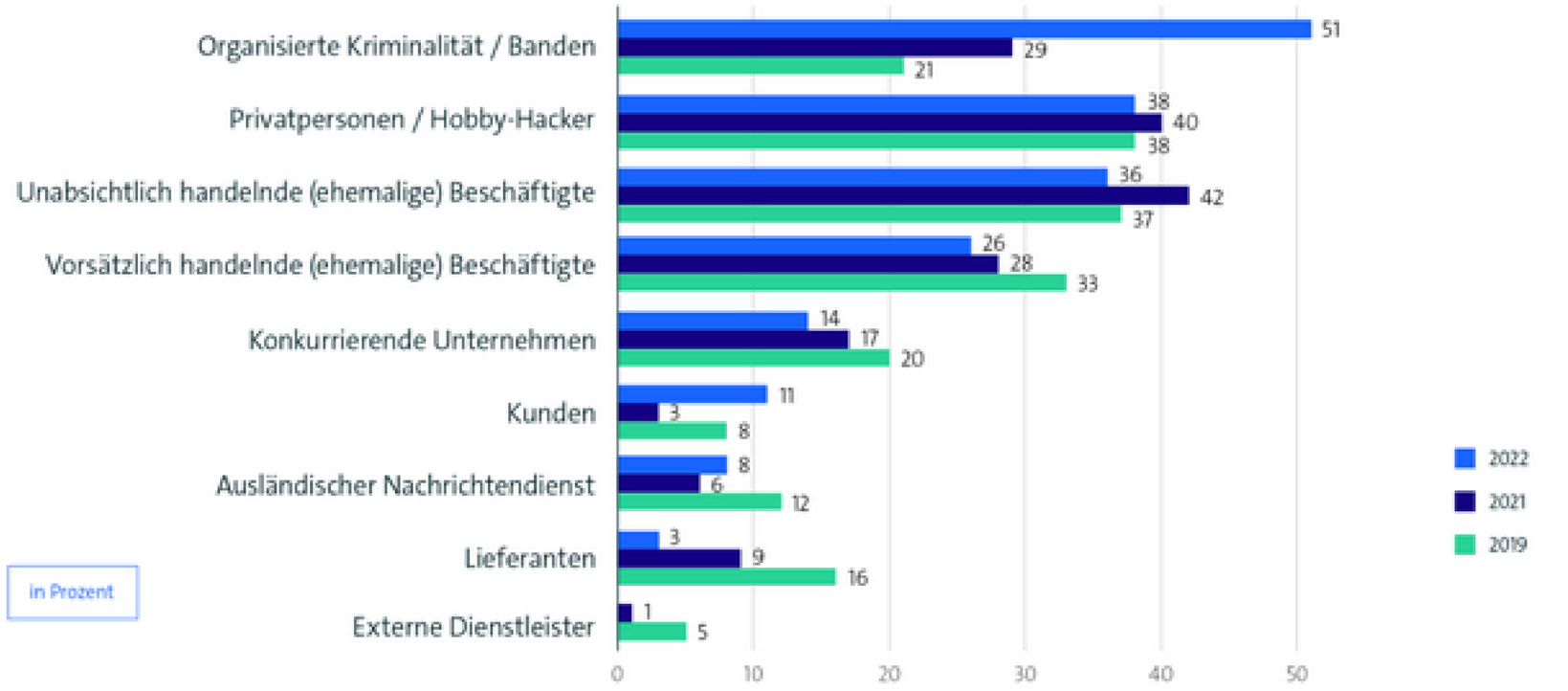
Greybox-Pentest

- ausgewogen
- effizient
- variable Tiefe

Warum ist das so wichtig?

Attacken auf die Wirtschaft werden professioneller

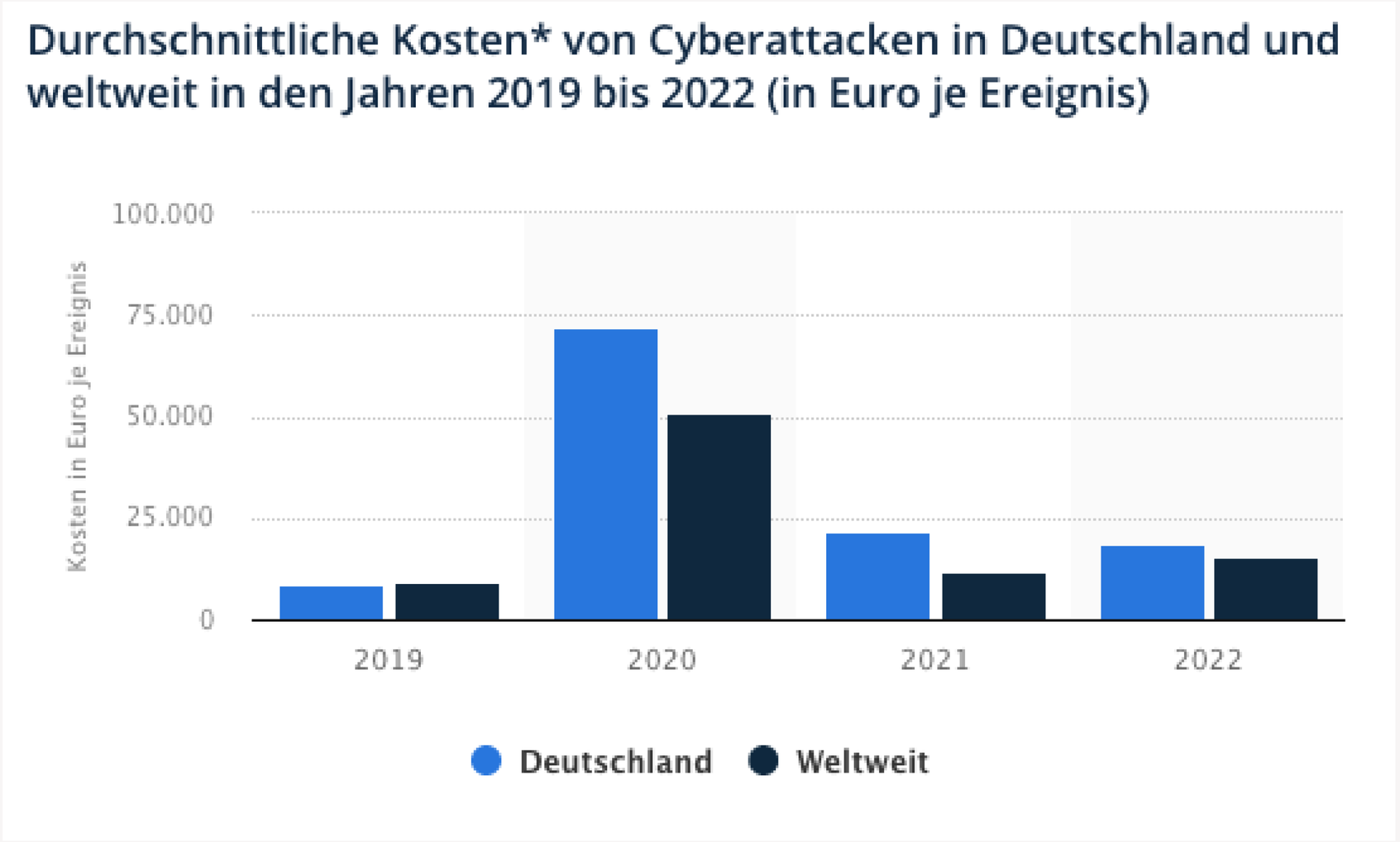
Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?



Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=915; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Warum ist das so wichtig?



Die versteckten Kosten eines Cyberangriffs
Was Cyberversicherungen gerne verschweigen...

Nicht nur Geld steht auf dem Spiel:

- Reputation
- Vertrauen
- Wissensabfluss
- Marktanteil
- Haftung der Veranwortlichen (GF, IT-Leiter, ...)

Nur ein geschütztes Unternehmen ist ein erfolgreiches Unternehmen

Business Continuity und Reputationsschutz

In der heutigen Geschäftswelt ist der Schutz von Daten nicht nur eine IT-Frage, sondern eine Priorität für das gesamte Unternehmen. Ein Datenleck kann das Vertrauen zerstören, das Jahre zum Aufbau benötigt hat.

Global verursacht ein Datenleck ca. 4,3 Millionen Euro Schaden bei allen Beteiligten

60 % der Unternehmen müssen aufgrund der verlorenen Reputation ihr Geschäft aufgeben.

Rechtliche Anforderungen

- DSGVO (Datenschutz-Grundverordnung)
- ISO-Norm 27001:2023 (A 8.29, A 12.6.1)
- BSI-Gesetz (Bundesamt für Sicherheit in der Informationstechnik)
- IT-Sig 2.0 (IT-Sicherheitsgesetz)
- TISAX (Trusted Information Security Assessment Exchange)
- TKG (Telekommunikationsgesetz)
- Weitere branchenspezifische Regelungen,

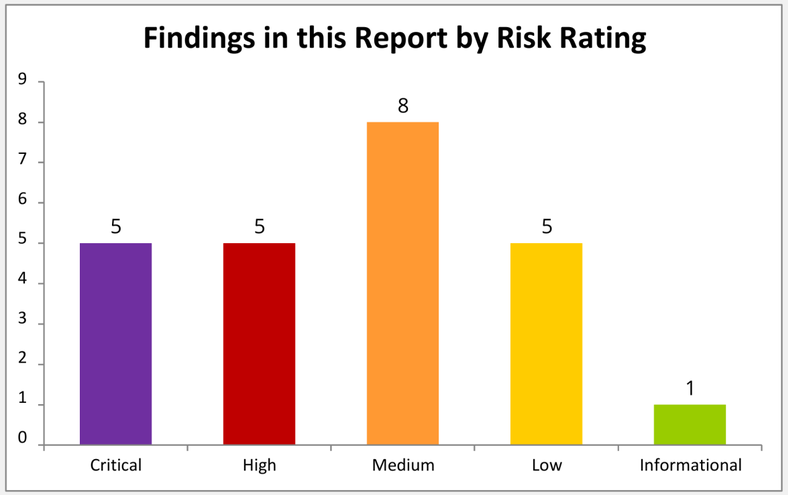
  z. B. für Finanzdienstleister, Gesundheitswesen, etc.

Pentest Report

Wie sieht ein Bericht aus? Was kann ich erwarten?

- Zusammenfassung (in nicht technischer Sprache für Unternehmer/Geschäftsführung)
- Überblick über die Verteilung der Schwachstellen
- Einstufung der Schweregrade der gefundenen Schwachstellen
- technische Details zu einzelnen Schwachstellen
  - CVSS Vektor und Schweregrad
  - Beschreibung
  - Lösungsvorschlag
- Erklärung der verwendeten Methodik und Tools

Vulnerability Assessment Report for
Client X



CVSS Score Range	Risk Rating	Number of Findings
9.0 to 10.0	Critical	5
7.0 to 8.9	High	5
4.0 to 6.9	Medium	8
0.1 to 3.9	Low	5
n/a	Informational	1

Detailed Internal Findings

Finding	Risk Rating	Affected Hosts
Apache < 2.4.49 Multiple Vulnerabilities	Critical	10.11.2.85
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Critical	10.11.2.85
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Critical	10.11.2.85
PHP Unsupported Version Detection	Critical	10.11.2.85
Unsupported Windows OS (remote)	Critical	10.11.2.30
Apache >= 2.4.17 < 2.4.49 mod_http2	High	10.11.2.85
Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi	High	10.11.2.85
PHP < 7.3.24 Multiple Vulnerabilities	High	10.11.2.85
PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	High	10.11.2.85
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	High	10.11.2.30
Apache >= 2.4.17 < 2.4.49 mod_http2	High	10.11.2.85
Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi	High	10.11.2.85
PHP < 7.3.24 Multiple Vulnerabilities	High	10.11.2.85
PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability	High	10.11.2.85
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	High	10.11.2.30
TLS Version 1.1 Protocol Deprecated	Medium	10.11.2.253
TLS Version 1.0 Protocol Detection	Medium	10.11.2.253
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	10.11.2.85
HTTP TRACE / TRACK Methods Allowed	Medium	10.11.2.85
SMB Signing not required	Medium	10.11.2.30

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Rating: High

CVSS Score: 8.1

CVSS Vector : CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

The remote Windows host is affected by the following vulnerabilities:

• Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

• An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in

SQL Dump Files Disclosed via Web Server

Rating: Medium

CVSS Score: 5.0

CVSS Vector: n/a

Description

The remote web server hosts publicly available files that contain SQL instructions. These files are most likely database dumps and may contain sensitive information.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

References

n/a

Hosts affected: 10.11.2.85

Evidence for 10.11.2.85

Location: tcp/8000

```
The following SQL files are available on the remote server :

- /db/onlinecourse.sql
```

Auswahl eines Penetrationstesting-Unternehmens

Auswahlkriterien:

- Qualifiziertes Personal
- Aktualität der Methoden
- Klare Kommunikation
- Anpassungsfähigkeit
- Vertraulichkeit
- Referenzen

Auswahl eines Penetrationstesting-Unternehmens

Zertifikate:

- Offensive Security Zertifikat:
  - OSCE
  - OSEP
- CISSP
- Bedingt: CEH (Theorie), OSCP (Einsteiger)

Auswahl eines Penetrationstesting-Unternehmens

- Billigangebote
  - Subunternehmer (im Ausland)
  - automatische Methoden
  - oberflächlich
- fehlende oder keine Berichte
- keine Referenzen
- zu schnelle Ergebnisse
- “Up-Seller”
  - Datenschützer
  - Systemhäuser

Vertragsdetails

Klärung von:

- Haftungsbegrenzung
- Haftung nach Art des Schadens - direkte vs. indirekte Schäden
- Versicherungsnachweis
- Abgrenzung der Verantwortlichkeiten
- Datenschutz

Ihre Gelegenheit, tiefer zu graben…

Expertenantworten auf Ihre brennendsten Fragen

Bleiben Sie verbunden und informiert

Ihr Aktionsplan: Die nächsten Schritte zur Sicherung

BSI Grundschutz

820 Seiten Kompendium

Linkedin Profil

3x pro Woche aktuelle News und Best Practices

Anmeldung zum Newsletter

1x pro Woche ausführliche Informationen

BreakinLabs

Vielen Dank!

BreakinLabs GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Thomas Moosmüller

Kontakt: thomas.moosmueller@breakinlabs.com