TEAL
ALWAYS CHALLENGING IT

Wenn die Forensiker gehen…

Überleben und Wiederaufbau nach dem Ransomware-Angriff

Teal Technology Consulting GmbH

Der Ablauf

Dienstag, 17:00 Uhr

Kontaktaufnahme durch Partnerunternehmen (Forensiker)

Dienstag

Mittwoch Morgen

Mittwoch, 07:30 Uhr

Termin mit der Kunden-IT

Mittwoch Vormittag

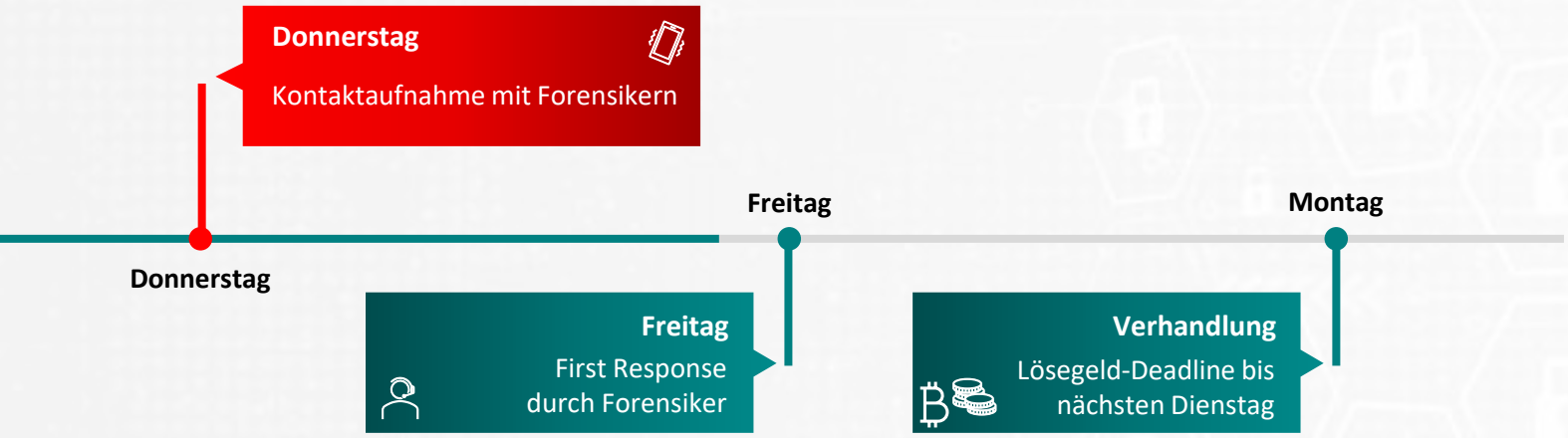
Mittwoch, 09:00 Uhr

Termin mit der Geschäftsführung

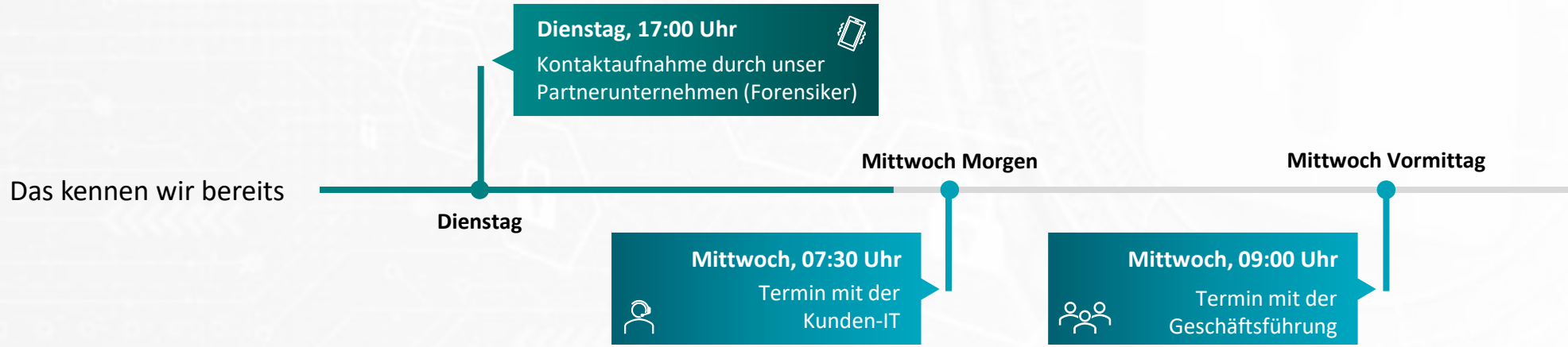
TEAL
ALWAYS CHALLENGING IT

Der Ablauf

1. Woche nach Kenntnisnahme des Angriffs



2. Woche nach Kenntnisnahme des Angriffs



TEAL
ALWAYS CHALLENGING IT

Der Ablauf

1. Woche nach Kenntnisnahme des Angriffs

Donnerstag
Kontaktaufnahme mit Forensikern

Donnerstag — **Freitag** — **Montag**

Freitag
First Response durch Forensiker

Verhandlung
Lösegeld-Deadline bis nächsten Dienstag

2. Woche nach Kenntnisnahme des Angriffs

Dienstag, 17:00 Uhr
Kontaktaufnahme durch unser Partnerunternehmen (Forensiker)

Dienstag — **Mittwoch Morgen** — **Mittwoch Vormittag** — **Mittwoch Mittag**

Mittwoch, 07:30 Uhr
Termin mit der Kunden-IT

Mittwoch, 09:00 Uhr
Termin mit der Geschäftsführung

Mittwoch, 12:00 Uhr
TEAM TEAL an der Arbeit beim Kunden

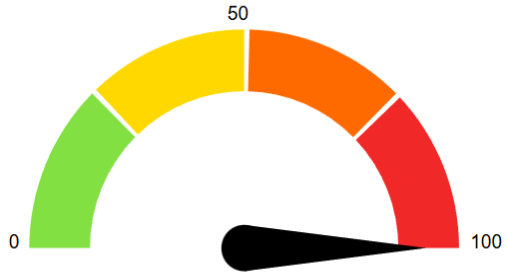
TEAL
ALWAYS CHALLENGING IT

PingCastle: Aktuelle Situation

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

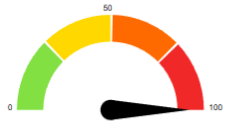
Compare with statistics

Privacy notice

Stale Object : 68 /100

It is about operations related to user or computer objects

15 rules matched



Privileged Accounts : 100 /100

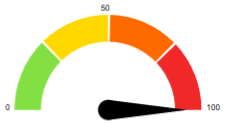
It is about administrators of the Active Directory

13 rules matched

Trusts : 20 /100

It is about connections between two Active Directories

1 rules matched



Anomalies : 100 /100

It is about specific security control points

23 rules matched

Wesentliche Ergebnisse

- Vielzahl von **GPOs** kann von jedem modifiziert werden
- **Login Scripte** können von jedem modifiziert werden
- **Domain Admins** mit Never Expiring Passwörter
- **Accounts mit Never Expiring** Passwörtern
- **Windows Server 2008 / 2012** vorhanden
- **Klartext Passwörter** in GPOs
- **Kerberos Passwort** ist sehr alt
- **Zertifikate Templates**, bei denen das "Subject" frei gewählt werden kann
- **Spooler Service** auf DC ist remote erreichbar

TEAL ALWAYS CHALLENGING IT

Aufgabe und Arbeitsweise TEAL

- Remote Zugriff
- Secure SharePoint zum Datenaustausch
- Kommunikation via Teams und E-Mail
- Maßnahmen definieren
  - **Tool Pingcastle zeigt, welche Schwachstellen es alles gibt** (vor allem im AD) → Schwachstellen abarbeiten und sicherstellen, dass die Sicherheitslücken geschlossen werden
  - **Bloodhound Scan**
- **Fokus:** Infrastrukturabsicherung, schnelle Lösungen, schließen der großen Lücken
- **Ziel:** Die Angreifer dürfen nicht mehr rein kommen

Was haben wir erreicht

PKI abgesichert

Absicherung der Public Key Infrastructure (PKI) und Bereinigung unsicherer Zertifikatskonfigurationen.

Verhindert den Missbrauch von Zertifikaten und schließt einen häufig genutzten Angriffsvektor im Active Directory.

Passwortwechsel durchgeführt

Umfassender Wechsel kompromittierter bzw. potenziell kompromittierter Passwörter.

Unterbricht bestehende Angreiferzugänge und stellt sicher, dass alte Zugangsdaten nicht weiter missbraucht werden können.

Accounts & Berechtigungen bereinigt

Aufräumen von Benutzer- und Service-Accounts, Entfernen unnötiger Adminrechte sowie nicht mehr benötigter Konten.

Deutlich reduzierte Angriffsfläche und geringere Möglichkeiten zur lateralen Bewegung im Netzwerk.

Exchange Mailflow in Cloud verlagert

Verlagerung des Mailflows in die Cloud zur Nutzung moderner Sicherheitsmechanismen.

Besserer Schutz vor Phishing, Malware und Social Engineering sowie erhöhte Transparenz und Kontrolle über den E-Mail-Verkehr.

Mailflow kann im Notfall mit einem Klick von der on-prem Infrastruktur abgekoppelt werden.

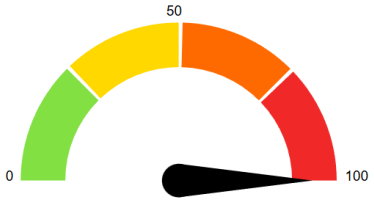
PingCastle Vergleich: vorher-nachher

vorher

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

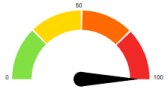
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Stale Object : 68 /100 — 15 rules matched

It is about operations related to user or computer objects



Privileged Accounts : 100 /100 — 13 rules matched

It is about administrators of the Active Directory

Trusts : 20 /100 — 1 rules matched

It is about connections between two Active Directories

Anomalies : 100 /100 — 23 rules matched

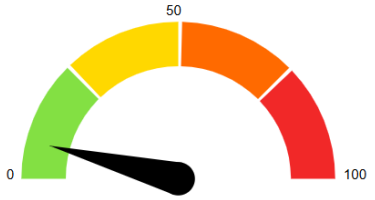
It is about specific security control points

nachher

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 8 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Stale Object : 8 /100 — 10 rules matched

It is about operations related to user or computer objects

Privileged Accounts : 1 /100 — 3 rules matched

It is about administrators of the Active Directory

Trusts : 0 /100 — 0 rules matched

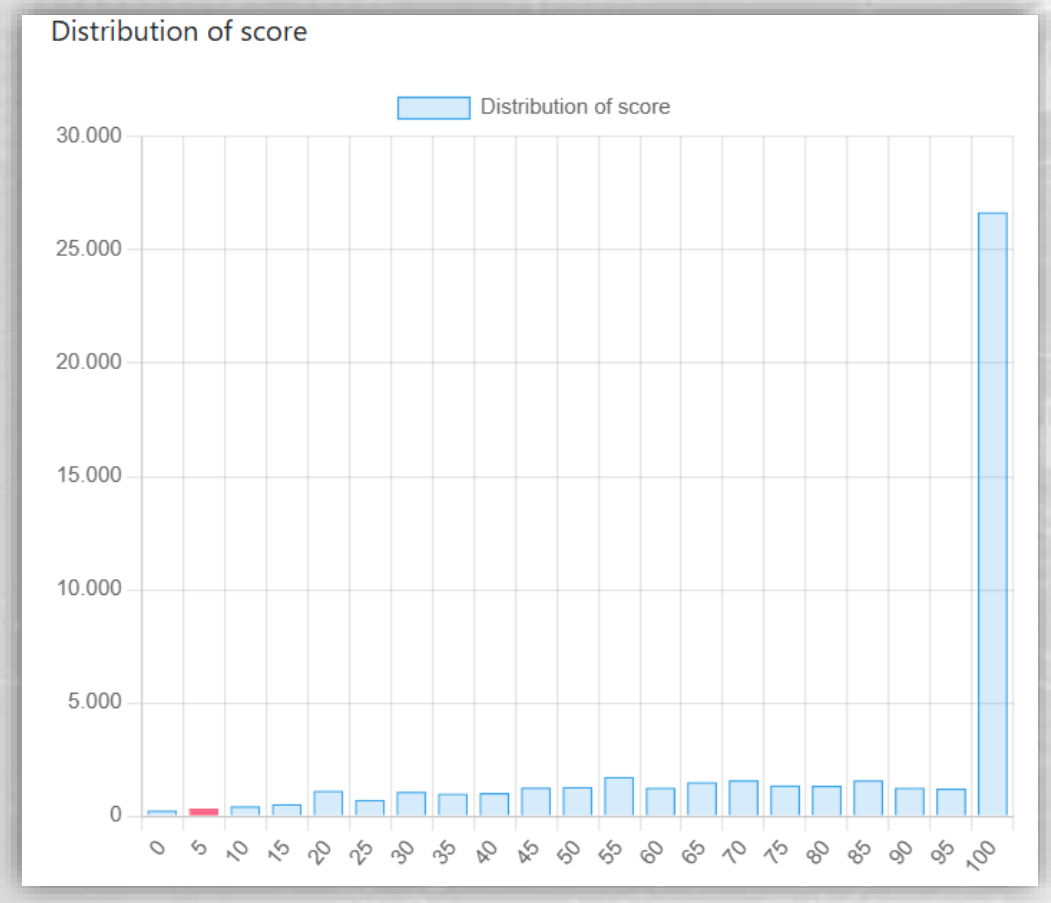
It is about connections between two Active Directories

Anomalies : 4 /100 — 13 rules matched

It is about specific security control points

TEAL ALWAYS CHALLENGING IT

PingCastle Vergleich: vorher-nachher



Mit einem PingCastle-Score von 8 gehört die Active-Directory-Umgebung **zu den besten 1,2 % der über 48.000 Domains**, die im Rahmen von PingCastle-Analysen miteinander verglichen werden.

Der Ablauf

Vor dem Angriff

Fehlende Priorisierung von IT-Sicherheit (sowohl in der Infrastruktur/technisch als auch menschlich)

Eintrittsvektor über **Social Engineering** per Telefon, dem Sender einer verschlüsselten ZIP und die Ausführung eines Executables

Der Ablauf

2 Monate nach Kenntnisnahme des Angriffs

Zielbild Workshop

seither

Infrastrukturabsicherung

Kontinuierliches Aufbauen und Optimieren einer nachhaltigen IT-Infrastruktur und IT-Sicherheit

TEAL ALWAYS CHALLENGING IT

Lessons Learned

Omnipräsenz

Ziel: Dem Kunden das Gefühl geben, dass wir "permanent da" sind

- Kurze Antwortzeiten
- kurzfristige Terminfindung
- kontinuierliche Statusupdates

Kommunikation

Ziel: Transparente Kommunikation und Statusupdates, um Vertrauen zu schaffen

Intern:
- Schnelle Abstimmung via Teams Chat
- Daily Sync Calls

Extern:
- Schnelle Abstimmung via Teams Chat
- Aufgabenübersicht via MS Planner
- Tägliche Status-Telefonate mit dem IT-Verantwortlichen
- Regelmäßige Updates an den Projekt-Sponsor (High-Level)

Standardisiertes und pragmatisches Vorgehen

Ziel: Durch standardisierte Strukturen maximale Geschwindigkeit ermöglichen

- Schwachstellenliste (z. B. aus PingCastle und/oder Bloodhound Scan) als pragmatischen Projektplan nutzen
- Standardreihenfolge nutzen

Technische Voraussetzungen und Dokumentation

Ziel: Arbeitsfähigkeit und Nachvollziehbarkeit sicherstellen

- Sicherstellen, dass jedes Projektmitglied die benötigten Zugänge hat
- Saubere Dokumentation der Maßnahmen (mehr als nur Stichpunkte/Schlagwörter in der Excel)
- Meetingprotokolle und Updates gut dokumentiert und strukturiert für den Kunden aufbereiten

UNSERE LEISTUNGEN AUF EINEN BLICK

Wir unterstützen Sie, wenn Sie…

- …verborgene Sicherheitsrisiken und passende Maßnahmen identifizieren möchten.
- …regulatorische Prozesse bedienen und Nachweise erbringen müssen.
- …nach einer Cyber-Attacke die nächsten Schritte planen.
- …Ihr Active Directory oder Azure sicher konfigurieren wollen.

Standard-Konzepte und jahrelange Erfahrung

- Tieringmodell
- Sichere Administration (PAW)
- Least Privilege Principle
- Clean-Source-Prinzip
- Systemhärtung
- Attack-Path-Management
- Rollen- & Rechtemodelle
- SIEM
- SCAMA (on-prem MFA)
- Vulnerability Management
- Infrastruktur-Management
- Hypervisor-Absicherung
- Exchange-Absicherung
- User & Software Lifecycle Management

… as a Service

- Systemhärtung
- Secure Active Directory
- Health- & Compliance check
- MDR
- PKI

Spezialisten für…

- Active Directory
- LAPS /Credential Guard
- Microsoft Server & Client Systeme
- Exchange
- Microsoft PKI
- Microsoft Hyper-V

- Azure
- Entra ID
- Azure MFA
- Intune
- Sentinel
- Defender Suite
- Azure Backup

- BloodHound (Enterprise)
- Enforce Administrator

TEAL ALWAYS CHALLENGING IT

Danke!

Gibt es noch Fragen?

Kontaktdaten

E-Mail: alexa.dippold@teal-consulting.de

E-Mail: fabian.boehm@teal-consulting.de

Web: https://www.teal-consulting.de/

Telefon: 0211/93675225

TEAL
ALWAYS CHALLENGING IT