pegasus IT
Member of ITventive Group

Security Quick Checks mit Open Source Instrumenten

pegasus IT
Member of ITventive Group

Alexander Karls
Cloud- und Security-Consultant
Mail: a.karls@pegasus-gmbh.de
Tel.: +49 9402 503-214

Kurzprofil:

- Über 20 Jahre in der IT tätig
- Mehr als 15 Jahre Erfahrung in leitender Funktion
- Langjährige Erfahrung aus selbständiger Tätigkeit
- Vorfall-Experte im CSN des BSI
- Erfahrener Trainer und Coach
- Podcast-Host von BlueScreen – Der Tech-Podcast

Allianz für Cyber-Sicherheit
Teilnehmer

Mitarbeiterzahl	100
Zertifizierung (pegasus)	ISO 9001 / 27001 / 27018
Standorte	Regenstauf (pegasus GmbH / pegasus IT / IQ) Ludwigsburg (EVIATEC Systems AG) Bern (EVIATEC Digital Solutions AG) Brøndby / Koppenh. (EVIATEC Scandinavia ApS)
Rechenzentren	3
Einsatzgebiet	Europaweit / Weltweit
Vernetzung	> 1500 Standorte weltweit
Geschützte Anwender	> 50.000
Server im RZ	> 500
Kundengröße / Schnitt	25 - 1000

Regensburg / DE

Ludwigsburg / DE

Bern / CH

Koppenhagen / DK

pegasus IT
Member of ITventive Group

Cyber Security: News und Trends

Cyber Security News und Trends

Golem.de

DDoS-Angriffe: Hacker legen Webseiten mehrerer deutscher Städte lahm - Golem.de

DDoS-Angriffe: Hacker legen Webseiten mehrerer deutscher Städte lahm. Mehrere deutsche Städte hatten in den letzten Tagen mit DDoS-Angriffen zu...

vor 4 Wochen

ComputerBase

Cyberwar: DDoS-Angriffe legen Webseiten deutscher Städte lahm

Webportale gleich mehrerer deutscher Städte waren in dieser Woche Ziele von DDoS-Angriffen und infolgedessen unerreichbar.

vor 4 Wochen

Hessenschau

Hackerangriffe in Frankfurt: Webseite der Stadt stundenlang offline, Uniklinikum noch immer betroffen

Stundenlang konnte am Donnerstag die Internetseite der Stadt Frankfurt nicht aufgerufen werden. Auch das Frankfurter Uniklinikum kämpft noch...

vor 4 Wochen

Tagesspiegel Background

+ Internet Governance Forum: Mehr New York, weniger Genf? +

Erstmals in der Geschichte des Internet Governance Forum (IGF) hat ein amtierender Präsident der UN-Generalversammlung bei der Konferenz...

vor 3 Wochen

T-Online

Nürnberg: Hacker bringen Webseite der Stadt mit Cyberattacke zum Absturz

Teilweise war die Seite der Stadt Nürnberg im Internet gar nicht mehr erreichbar. Hacker hatten die Server angegriffen und in die Knie...

vor 1 Monat

Siegener Zeitung

Siegen: Hackerangriff auf Kommunen - welche Fortschritte hat die Südwestfalen IT zu vermelden?

Bei der Analyse des Hackerangriffs auf die Südwestfalen-IT (SIT) gibt es jetzt wohl Fortschritte. Die erste Phase der forensischen Analysen...

vor 1 Stunde

Neuigkeiten über Ransomware

Golem.de

Südwestfalen IT: Ransomware-Angriff legt Dienste deutscher Verwaltungen lahm -...

vor 2 Tagen

Westfalenpost

Hackerangriff: Wann die ersten Programme wieder laufen sollen

vor 3 Stunden

ComputerBase

Südwestfalen IT: Deutsche Verwaltungen durch Ransomware-Angriff gestört

vor 2 Tagen

FAZ

Hackerangriff auf Südwestfalen-IT: Was Sie über die Cyberattacke wissen müssen

Auto anmelden oder die Ehe beurkunden? Fehlanzeige. Was passiert, wenn Cyberkriminelle einen IT-Dienstleister schachmatt setzen.

vor 1 Tag

LokalPlus

In den Verwaltungen müssen 22.000 Computer überprüft

Kreis Olpe. Der durch den Cyberangriff auf die Südwestfalen-IT entstandene Schaden für die betroffenen Kreise, Städte und Gemeinden ist noch...

vor 22 Stunden

Quelle: Google

Cyber Security News und Trends

Ransomware ist und bleibt die größte Bedrohung

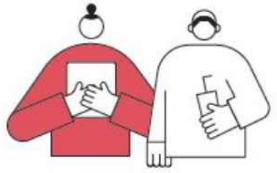
Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.

Download: Die Lage der IT-Sicherheit in Deutschland 2023

Cyberkriminalität wird professioneller

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service“ agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen.

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Online-Server	Schwachstellen, offene oder falsch konfigurierte Online-Server

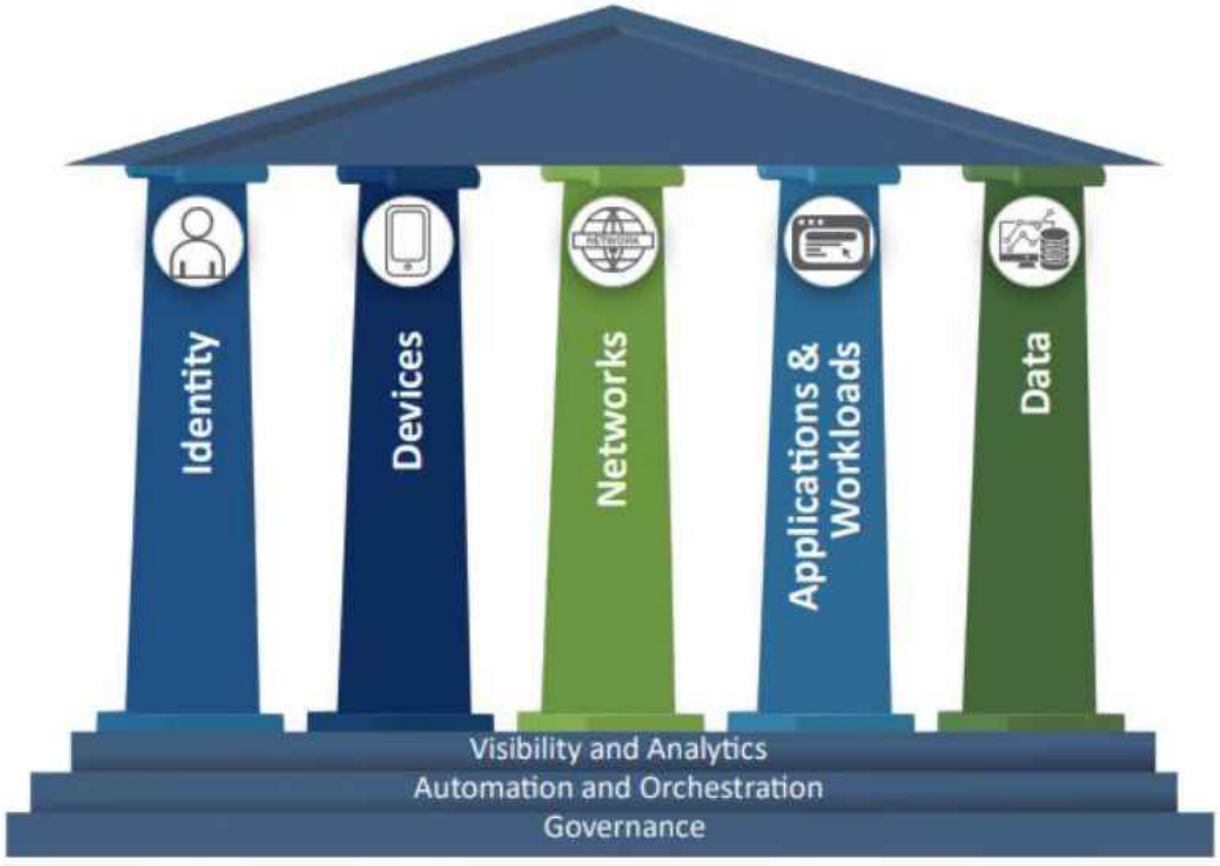
Quelle: BSI

pegasus IT
Member of ITventive Group

Know your Assets!

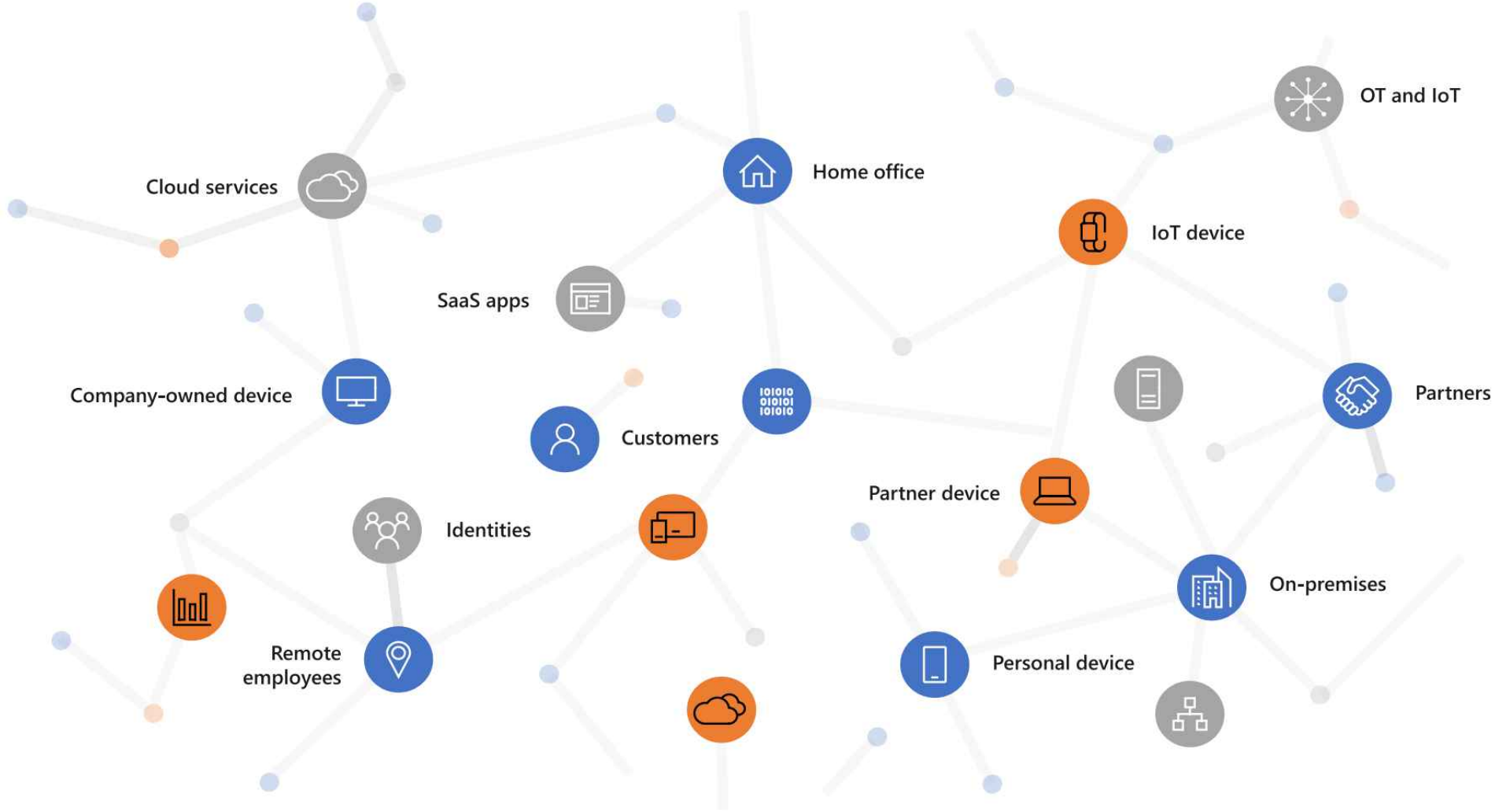
Know your Assets!

Erstellt mit MidJourney: cybercrime in a house



Quelle: CISO Guidelines Handbook

Know your Assets!



Quelle: Microsoft

pegasus IT
Member of ITventive Group

Übliche Schwach-stellen-Scans kosten Geld ☹

Schwachstellen-Scans im allgemeinen

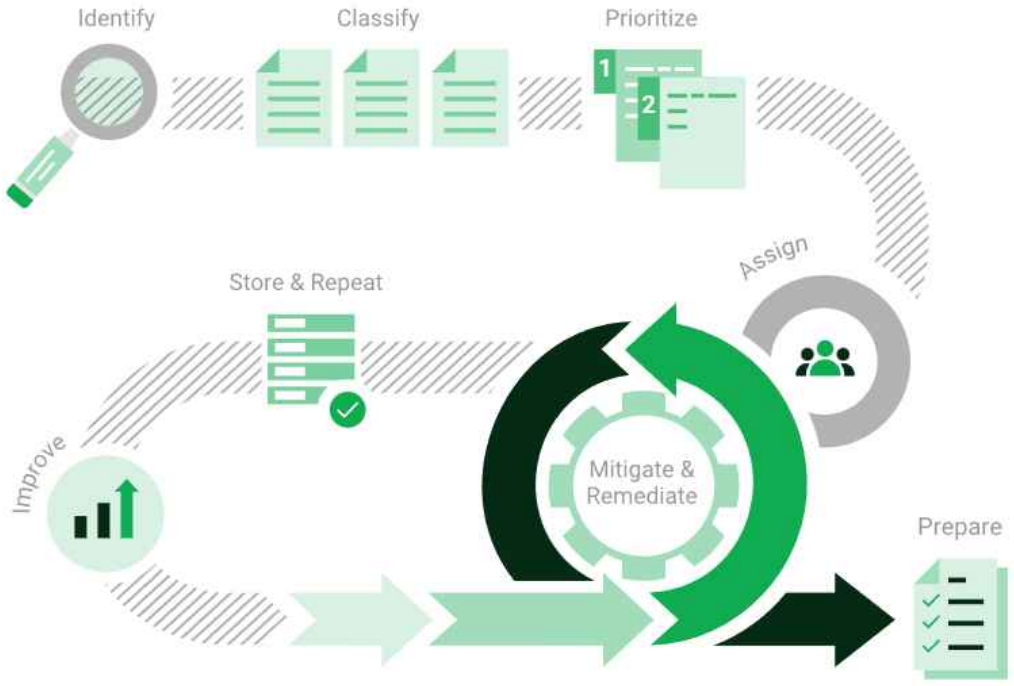


Abb. 1: Der Prozess

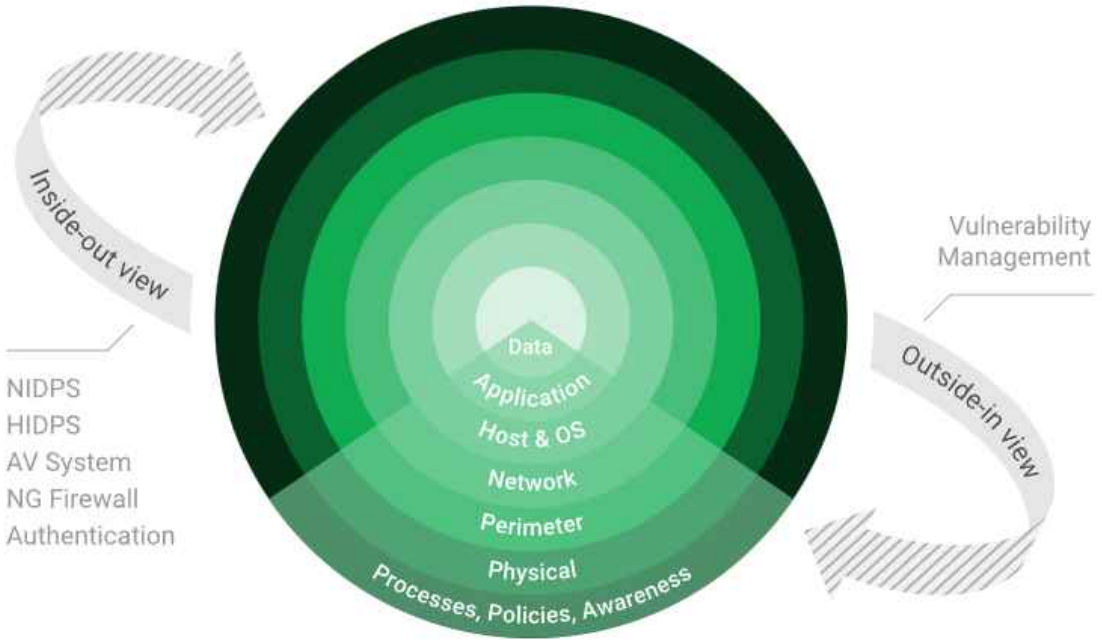


Abb. 2: Funktions-Schema

Quelle: Greenbone

Schwachstellen-Scans mit Greenbone MSP

Dashboard | Kachelübersicht | Tabellenübersicht

7.5

Scan external

Scanstart: 17.09.2022, 22:02
Scanende: 18.09.2022, 04:38
Scandauer: 6 Stunden, 35 Minuten, 47 Sekunden

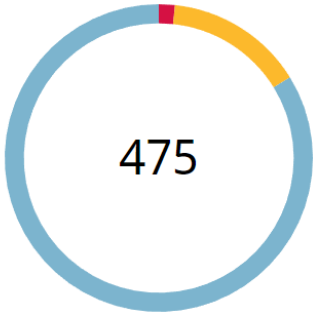
Schwachstellen insgesamt

475

Schwachstellen nach Lösungstyp

Temporary Fix Info	Risks Reduction Info	Official Fix Available	Searching For Fix	No Fix Available
13	65	17	0	380

Schwachstellen nach Schweregrad



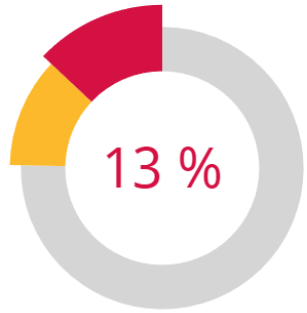
High	8
Medium	69
Low	398

Anteil der Schwachstellen, die mit einer Lösung behoben werden können

Temporary Fix
13 %

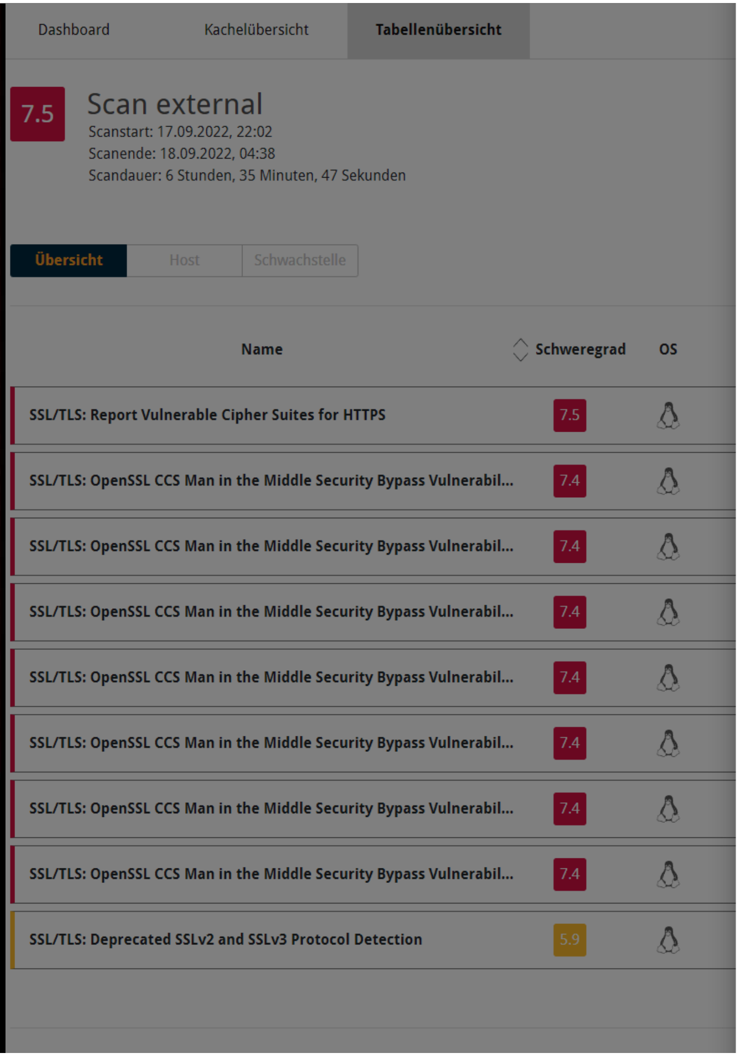
Risk Reduction
12 %

Temporary Fix	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Risk Reduction	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
other	



Quelle: Greenbone

Schwachstellen-Scans mit Greenbone MSP



SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Zusammenfassung

This routine reports all SSL/TLS cipher suites accepted by a service
where attack vectors exists only on HTTPS services.

Ergebnis zur Erkennung

```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_DHE_RSA_WITH_DES_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)
```

Lösung

Art der Lösung: Temporary Fix

The configuration of this services should be changed so
that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Betroffene Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Schwachstellen-Einblick

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Verweise

OTHER:

- CVE-2016-2183
- CVE-2016-6329
- CVE-2020-12872
- https://bettercrypto.org/
- https://mozilla.github.io/server-side-tls/ssl-config-generator/
- https://sweet32.info/

Quelle: Greenbone

pegasus IT
Member of ITventive Group

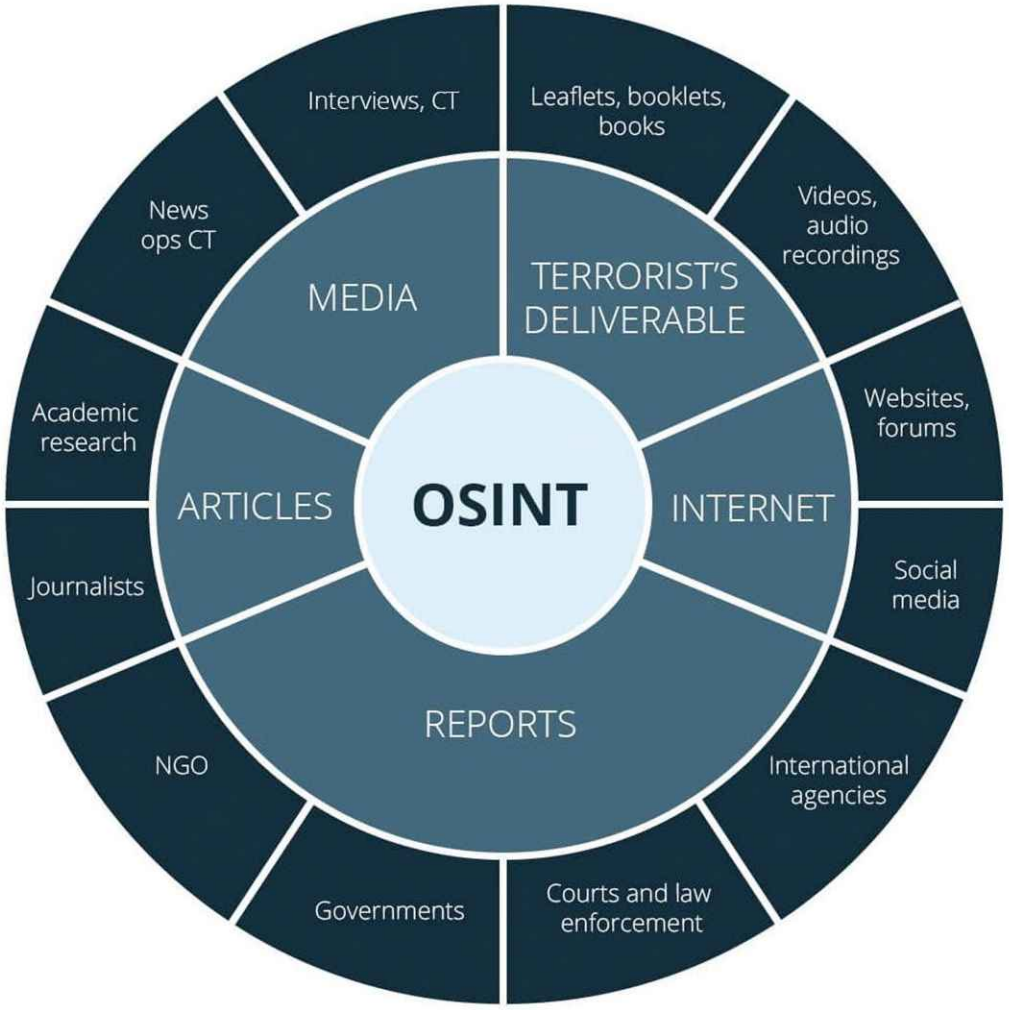
Technische Angriffsvektoren erkennen mit OSINT Werkzeugen

Was bedeutet OSINT?

„Open Source Intelligence (OSINT) ist ein Begriff aus der Welt der Nachrichtendienste und des Militärischen Nachrichtenwesens, bei dem für die Nachrichtengewinnung Informationen aus frei verfügbaren, offenen Quellen gesammelt werden, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen.

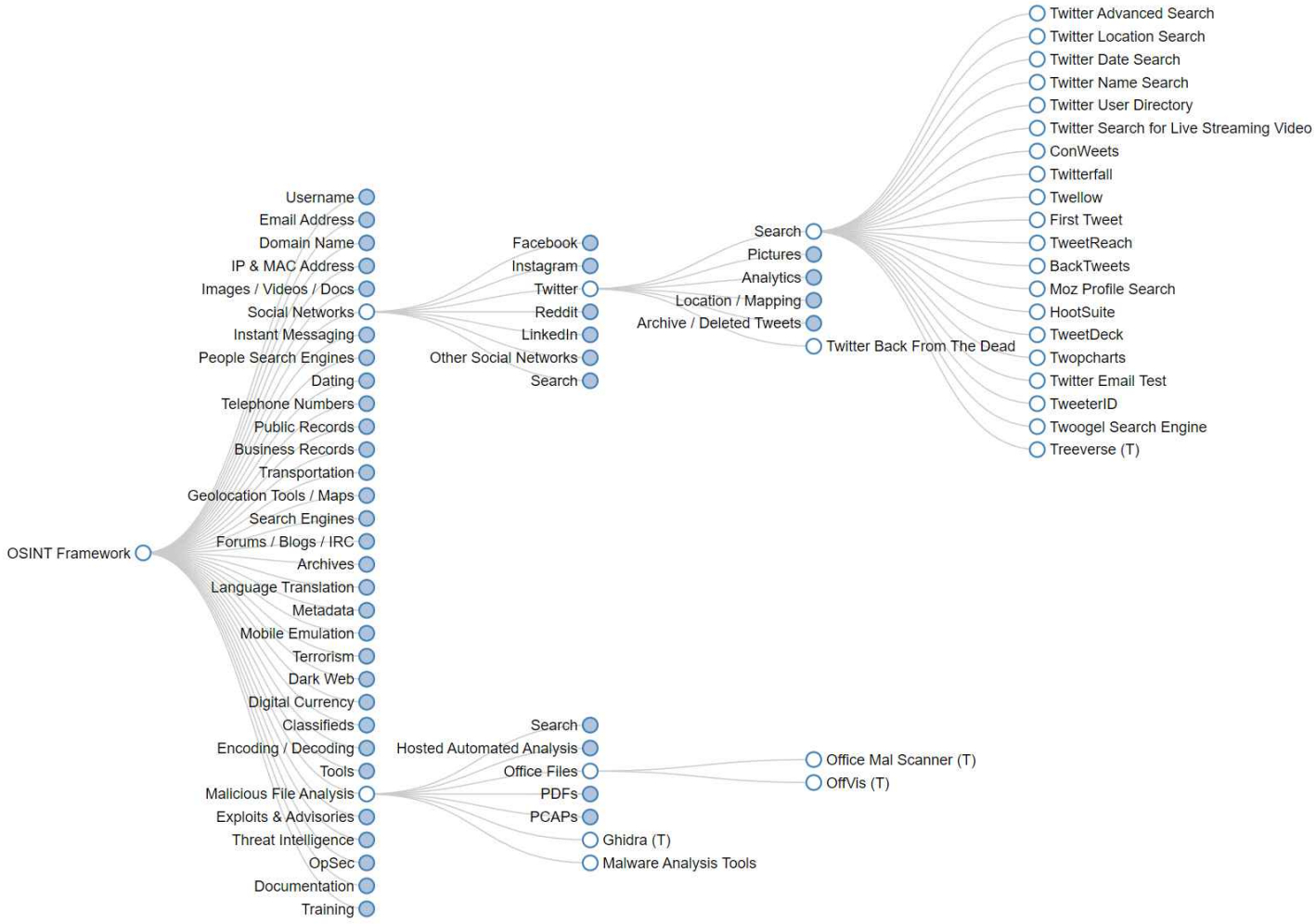
Dabei werden frei zugängliche Massenmedien genutzt, wie Printmedien, Rundfunk sowie das Internet und Web-basierte Anwendungen wie Google Earth. Der begriffliche Bezug auf Open Source bedeutet, dass frei zugängliche Informationen genutzt werden; eine Verbindung zu Open-Source-Software besteht nicht.“

Quelle: Wikipedia



Quelle: Medium / Data Driven Inspector

Das OSINT Framework



"OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost."

Quelle: https://osintframework.com/

Welche Informationen liefert OSINT?

Beispiele:

Extrakte aus dem Domain Name System (DNS):
- Hostnamen
- IP Adressen
- Kontaktdaten und Rufnummern
- Security Challenges
- Genutzte Dienste
- Informationen zu Security Settings (DNSSEC, Zonen Transfer, Wildcard Resolution..)
- E-Mail-Security Einstellungen

Werkzeuge: DNSRecon, DNSEnum, WTFIS, Robtex

Extrakte aus Domain-Registern und allg. verfügbaren Datenbanken:
- Registrar
- Anschrift
- Letzte Änderung
- Technische Ansprechpartern (Admin-C)
- ISP und Hoster
- Bekannte Probleme

Werkzeuge: WTFIS, Virustotal-DB, Passivetotal, Greynoise

Welche Informationen liefert OSINT?

Beispiele:

Konkrete Extrakte aus Shodan, der „Suchmaschine für Hacker“:
- Genutzte Anwendungen
- Software-Versionen
- Offene Ports
- Erreichbare Systeme und Anwendungen (OWA, ECP, RDP..!)
- Verwendete Zertifikate inkl. Trust-Zustand (Self signed, Public signed)
- Verschlüsselungs-Algorithmus und Schlüssellänge der Zertifikate
- Schwachstellen inkl. CVE-Verweisen
- …

Werkzeuge: Shodan.io, Shodan API

Weitere Beispiele:
- Extrakte aus Blacklist-Registern und –Datenbanken mit InfoOoze
- Benutzernamen und verwendete Dienste mit NameCHK
-Personen- und Domainsuche mit Hunter.io
- Metadaten aus Dokumenten wie Namen, Organisation, verwendete Software
- Metadaten aus Bildern / Fotos wie Modell der Kamera, Geo-Locationen…
- Versehentlich öffentlich erreichbare Webserver-Verzeichnisse mit GHDB und GoBuster

pegasus IT
Member of ITventive Group

Live-Demo

Rechtliche Situation in Deutschland

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202c verweist insb. auf folgende Vorschriften:

§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Gericht sieht Nutzung von Klartext-Passwörtern als Hacken an

Der Programmierer, der eine gravierende Lücke in der Software der Firma Modern Solution aufgedeckt hat, fällt unter den Hackerparagrafen, meint das Gericht.

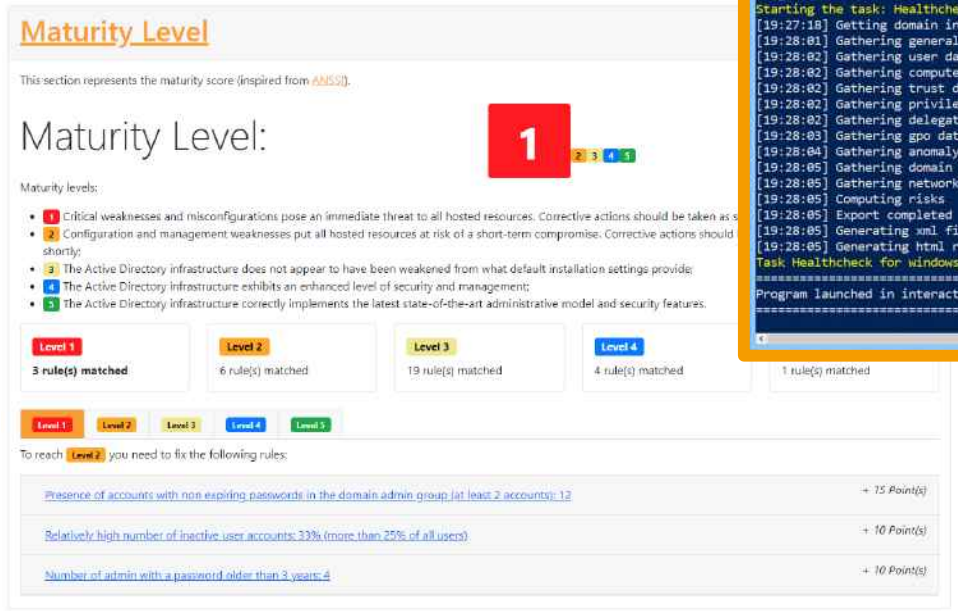
Lesezeit: **8 Min.** In Pocket speichern 820

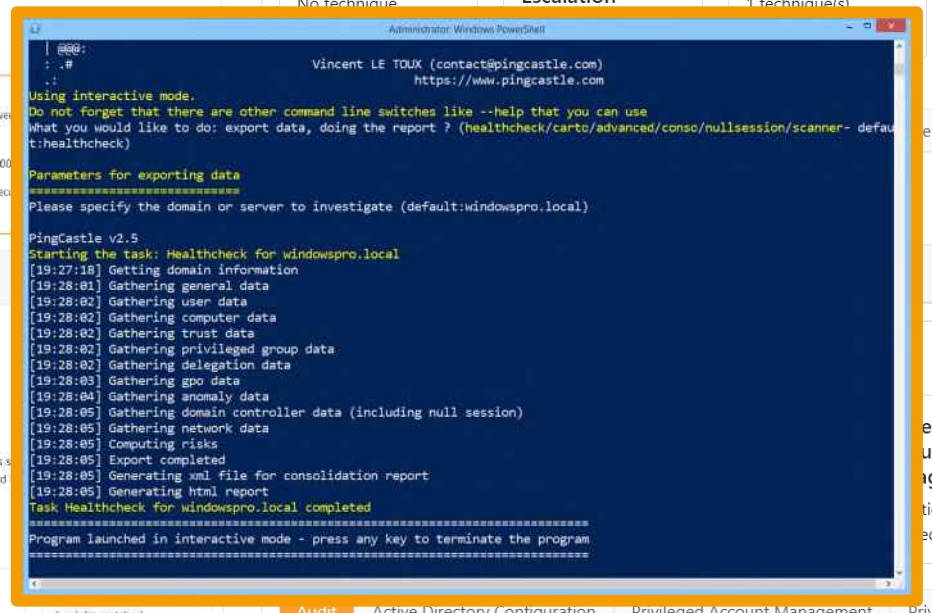
Vor dem beschaulichen Amtsgericht in Jülich wurde ein Prozess verhandelt, der die Gefahren verdeutlicht, denen sich Menschen mitunter aussetzen, die versuchen, Sicherheitslücken in der Software deutscher Firmen zu finden. (Bild: Fabian A. Scherschel)

pegasus IT
Member of ITventive Group

Active Directory Assessments mit PingCastle

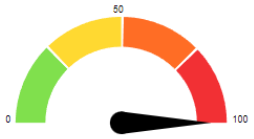
Active Directory Assessments mit PingCastle





Active Directory Assessments mit PingCastle

Anomalies analysis



Anomalies : 100 /100

It is about specific security control points

Anomalies rule details [17 rules matched on a total of 62]

Last change of the Kerberos password: 3813 day(s) ago *+ 50 Point(s)*

Mitigate golden ticket attack via a regular change of the krbtgt password

Rule ID:
A-Krbtgt

Description:
The purpose is to alert when the password for the krbtgt account can be used to compromise the whole domain. This password can be used to sign every kerberos ticket. Monitoring it closely often mitigates the risk of golden ticket attacks greatly.

Technical explanation:
Kerberos is an authentication protocol. It is using to sign its tickets a secret stored as the password of the krbtgt account. If the hash of the password of the krbtgt account is retrieved, it can be use to generate authentication tickets at will.
To mitigate this attack, it is recommended to change the krbtgt password between 40 days and 6 months. If it not the case, every backup done until the last password change of the krbtgt account can be used to emit Golden tickets, compromising the entire domain.
Retrieval of this secret is one of the highest priority in an attack, as this password is rarely changed and offer a long term backdoor.
Also this attack can be performed using the former password of the krbtgt account. That's why the krbtgt password should be changed twice to invalidate its leak.

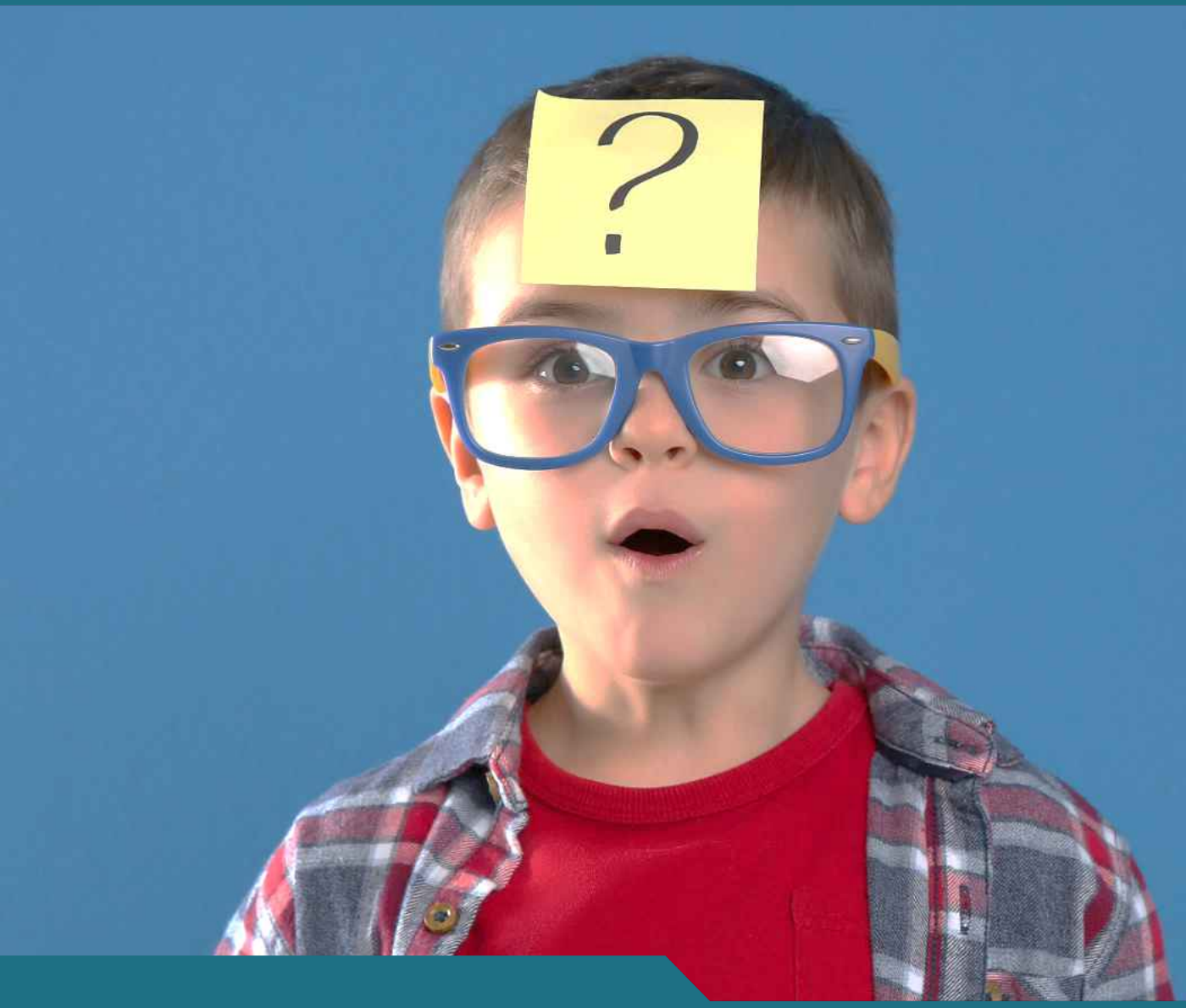
Advised solution:
The password of the krbtgt account should be changed twice to invalidate the golden ticket attack.
Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers You should wait at least 10 hours between each krbtgt password change.

There are several possibilities to change the krbtgt password.
First, a Microsoft script can be run in order to guarantee the correct replication of these secrets. Unfortunately this script supports only English operating systems.
Second, a more manual way is to essentially reset the password manually once, then to wait 3 days, then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden ticket attack.

pegasus IT
Member of ITventive Group

Live-Demo

pegasus IT
Member of ITventive Group



Haben Sie Fragen oder Anregungen?

pegasus IT – Member of ITVentive Group

ITventive Group

eviatec Systems AG, Monreposstrasse 57, D-71634 Ludwigsburg
pegasus GmbH, Bayernstrasse 10, D-93128 Regenstauf
eviatec Digital Solutions AG, Uferweg 17, CH-3013 Bern
eviatec Scandinavia ApS, Park Alle 295, 2. floor, DK-2605 Brøndby

pegasus-gmbh.de