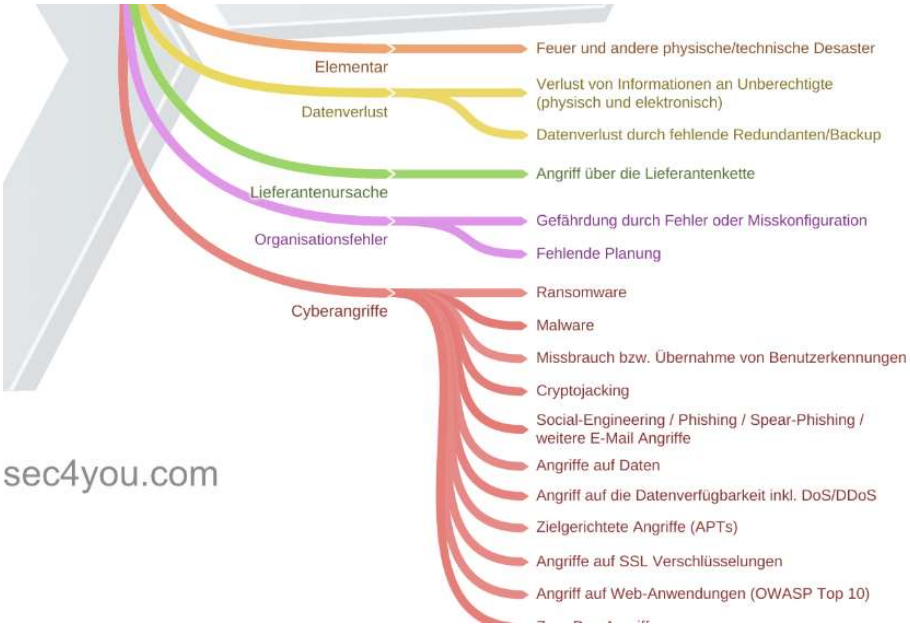
SEC4YOU
Advanced IT-Audit Services

! Dieser Artikel wurde 2024 überarbeitet und neu veröffentlicht.
Die neue Version finden Sie unter:
https://www.sec4you.com/informationssicherheitsrisiken-27001-tisax/

Erhebung Informationssicherheits-Risiken für 27001 und TISAX®



Erhebung Informationssicherheits-Risiken für 27001 und TISAX®

Jedes Unternehmen sollte aufgrund der rasant steigenden Gefahren für einen IT-Betrieb die relevanten IT-Gefährdungen in Bezug auf die Informationssicherheit erheben und bewerten. Jedoch ist die Auswahl der Gefährdungen (Threats) für die primären InfoSec Schutzziele Vertraulichkeit, Integrität und Verfügbareit sehr aufwendig, weil es speziell für kleine und mittelständische Unternehmen keine einfachen Bedrohungslisten gibt.

Dieser Aufgabe hat sich SEC4YOU angenommen und die SEC4YOU Informationssicherheits-Bedrohungsliste 2022 erstellt. In diesem Artikel werden die wichtigsten Bedrohungen vorgestellt und erläutert. Leser bekommen einen fundierten Überblick, gegen welche Gefahren Sie ihr Unternehmen abgesichert haben sollten, da diese mittlerweile fast täglich für Unternehmen zur Realität werden.

Was erreicht man durch eine Informationssicherheitsrisikobeurteilung?

Neben der Vermeidung erheblicher bis existenzbedrohender wirtschaftlicher sowie immaterieller Schäden, unterstützt eine Informationssicherheitsrisikobeurteilung die Auswahl geeigneter InfoSec Maßnahmen, die erforderlich sind das Unternehmen vor den Gefahren zu schützen. Sofern Sie ein ISMS nach ISO 27001 oder TISAX® betreiben, muss das Unternehmen das komplet-

Search

Suchen...

Recent Posts

- Umsetzung der Cyber Trust Austria Silber und Gold Label
- Effiziente Umsetzung der Cyber Trust Austria Label
- 30% Förderung für IT-Sicherheit und Informationssicherheit
- Lieferantenbewertung nach ISO 27001:2022
- Grundlegende Sicherheitsmaßnahmen für Passwörter

Categories

- Blog
- Blog
- Data protection
- Data protection - awareness
- Datenschutz
- Datenschutz-Awareness
- Events
- Hints
- ISMS tools

te Risiko-Assessment von der Risiko-Methode, den Beurteilungskriterien und der Beurteilung dokumentiert nachweisen.

Quellen für Informationssicherheits-Bedrohungen

Als Grundlage für die SEC4YOU Informationssicherheits-Bedrohungsliste 2022 wurden folgende Quellen genutzt:

Die 47 **Elementare Gefährdungen** des Deutschen Bundesamt für Informationssicherheit (BSI)

Eine sehr klassische Liste, die eine Vielzahl an Elementargefahren auflistet und sich intensiv mit den Aspekten Sabotage/Terror und Spionage beschäftigt. Leider werden in dieser Veröffentlichung die modernen Cyberangriffsvektoren nicht ausreichend bewertet.

ENISA Threat Landscape 2021

Eine wertvolle Bewertung der Informationssicherheit der Europäischen Agentur für Cybersecurity die auf 115 Seiten die Cybersecurity Trends analysiert und hierbei die wesentlichsten neun Gefährdungen beschreibt und detaillierte Empfehlungen zur Vermeidung gibt.

2022 Cyberthreat Defense Report der CyberEdge Group

Dieser Report beleuchtet Technologien und deren Resilienz gegen Cybergefahren, zusätzlich bietet der Report eine ausgezeichnete Bewertung von 12 Cybergefahren die in keiner Risikobeurteilung fehlen dürfen.

Klare Unterscheidung zwischen Gefährdung, Maßnahme, Wirkung und Wirksamkeitsprüfung

In einer Informationssicherheitsrisikobeurteilung ist der CISO gefordert tatsächlich die Gefahren/Gefährdungen zu bewerten und erst später die Maßnahme und deren mögliche Wirkung festzulegen, hier an einem vereinfachten Praxisbeispiel „Malware“ die Abgrenzung der Begriffe:

- **Gefährdung**: Die Gefahr, dass das Unternehmen von Malware infiziert wird.
- **Maßnahme**:
  - Flächendeckende Malware-Schutzsoftware auf allen Endgeräten mit Hersteller A
  - Perimeter Gateway-Schutz und Upload-Filter mit Hersteller B
  - Regelmäßige Prüfung interner und externer Dienste auf Schwachstellen (Vulnerabilities)
- **Wirkung der Maßnahme** (die Definition der Wirksamkeitsziele):
  - Malware aus der Quelle Internet und E-Mail wird zuverlässig am Gateway erkannt.
  - Malware aus der Quelle USB-Sticks und Ende-zu-Ende verschlüsselten E-Mails wird zuverlässig am Endgerät erkannt.
- **Wirksamkeitsprüfung**:
  - Gibt es Indizien, dass Malware am Gateway, Upload-Filter oder Endgeräten nicht zuverlässig erkannt werden?
  - Wird Malware auch in verschlüsselten Verbindungen erkannt?
  - Sofern in der Wirksamkeitsprüfung festgestellt wird, dass die Maßnahme die Wirksamkeit nicht erfüllen, müssen die Maßnahmen optimiert oder erweitert werden.

- ISMS Tools
- Tipps
- Uncategorized
- Veranstaltungen

Archiv

- April 2023
- März 2023
- Februar 2023
- November 2022
- Juli 2022
- Mai 2022
- November 2021
- August 2021
- Juli 2021
- Mai 2020
- November 2019
- Juni 2019
- Mai 2019
- Februar 2019
- Januar 2019
- September 2018
- April 2018
- März 2018
- Februar 2018
- Januar 2018
- Dezember 2017
- November 2017
- Oktober 2017
- September 2017
- Juli 2017
- Juni 2017
- April 2017

› Februar 2017

Die SEC4YOU Methodik

CyberEdge 2022 Cyberthreat Defense Report aufgelistet und priorisiert. Die **Priorität** einer Gefährdung erkennen Sie in der Grafik unten an der roten Flagge.

Dann haben wir die Gefährdungen in die folgenden **Kategorien** klassifiziert: Elementar, Datenverlust, Lieferantenursache, Terror/Insider/Sabotage/Spionage, Organisationsfehler, Cyberattacke

In einem **Filter** haben wir anschließend die priorisierten Gefährdungen aller 3 Quellen zusammengefasst, hierbei jedoch die Kategorie Terror/Insider/Sabotage/Spionage entfernt, weil für einen Großteil der Unternehmen diese Kategorie wenig relevant ist.

Das Ergebnis: Die SEC4YOU Informationssicherheits-Bedrohungsliste 2022

Die folgenden 17 Bedrohungen wurden als die wesentlichsten Gefahren für den IT-Betrieb erarbeitet:

Elementar

1. Feuer und andere physische/technische Desaster

Datenverlust

2. Verlust von Informationen an Unberechtigte (physisch und elektronisch)
3. Datenverlust durch fehlende Redundanzen/Backup

Lieferantenursache

4. Angriff über die Lieferantenkette

Organisationsfehler

5. Gefährdung durch Fehler oder Misskonfiguration
6. Fehlende Planung

Cyberangriffe

7. Ransomware
8. Malware
9. Missbrauch bzw. Übernahme von Benutzerkennungen
10. Cryptojacking
11. Social-Engineering / Phishing / Spear-Phishing / weitere E-Mail Angriffe
12. Angriffe auf Daten
13. Angriff auf die Datenverfügbarkeit inkl. DoS/DDoS
14. Zielgerichtete Angriffe (APTs)
15. Angriffe auf SSL Verschlüsselungen
16. Angriff auf Web-Anwendungen (OWASP Top 10)
17. Zero-Day Angriffe

Erklärung zu der Bedrohungsliste

Im Zuge der Informationssicherheitsrisikobeurteilung bewerten Sie die Bedrohungsliste mit den Asset-Gruppen und identifizieren bestehende und zusätzlich benötigte technische und organisatorische Maßnahmen. Nutzen Sie die Erklärungen unten für die Anwendung einer Risikobeurteilung nach Auswirkung und Eintrittswahrscheinlichkeit.

1. Feuer und andere physische/technische Desaster

Hierbei geht es um Naturkatastrophen und lokale Elementargefahren, wie Feuer oder Wasser die IT-Infrastrukturen zerstören können. Jedoch auch technische Defekte in Serverräumen oder an kritischen IT-Diensten die einen IT-Betrieb vollständig unterbrechen. Egal ob Hochwasser, ein Brand oder der Löschschaum das Server-Rack zerstört, sorgen sie rechtzeitig für Redundanzen und mehrfache Datenhaltung.

2. Verlust von Informationen an Unberechtigte (physisch und elektronisch)

Bei dieser Gefahr geht es um die Informationen selbst. Jedoch ist es unerheblich, ob eine unberechtigte Person diese als Papierdokumente entwendet, oder diese über einen Fernzugriff elektronisch kopiert werden. Die unternehmenskritischen Informationen in den Händen eines Mitbewerbers oder der Reputationsverlust kann dem Unternehmen nachhaltig schaden.

3. Datenverlust durch fehlende Redundanzen/Backup

Sofern kritische IT-Dienste nicht redundant ausgelegt sind (u.a. Storage, Virtualisierungsplattformen, Domain Controller, Verzeichnisdienste, DNS-Server, Web-Dienste) kann es zu Datenverlusten kommen. Hierbei können sowohl Hardwaredefekte als auch Konfigurationsfehler oder einfach menschliche Fehler die Ursache für einen Datenverlust sein. Schlussendlich hilft eine fachmännisch geplante und regelmäßig getestete Backup-Lösung vor Datenverlust.

4. Angriff über die Lieferantenkette

Bei der „Supply-Chain-Attack“ wird das Vertrauen zwischen einem (großen) Lieferanten und seinen Kunden missbraucht. Hier können Angreifer über eingerichtete Fernzugriffe oder beim Lieferanten hinterlegte Credentials bzw. Schlüssel die Daten und Systeme eines (oder vieler) Unternehmen kompromittieren. In der Vergangenheit wurden jedoch ein Großteil der Angriffe über kompromittierte Software einzelner Lieferanten durchgeführt, wo Hacker gezielt Angriffsmethoden in vermeintlich vertrauenswürdige Software-Updates platzieren konnten.

5. Gefährdung durch Fehler oder Misskonfiguration

Speziell durch fehlende Konfigurationsvorgaben (Hardening-Guidelines, Configuration-Baselines) und auch durch fehlende Automatisierungen werden Server und IT-Dienste unterschiedlich und z.T. unsicher konfiguriert. Auch werden nachträgliche sicherheitsrelevante Konfigurationsanpassungen durch die IT-Teams von Unternehmen oft nicht umgesetzt. Leider allzu oft werden Software oder Dienste mit den Standard-Konfigurationen und Default-Zugangsdaten in Betrieb genommen, was von Angreifern einfach ausgenutzt werden kann.

6. Fehlende Planung

Mangelhaft geplante IT-Infrastrukturen, unsachgemäße Wartungs- und Reparaturprozesse, unterschätzte IT-Migrationen, Beschaffung von IT-Systemen mit unzureichenden Sicherheitseigenschaften, schlechte Ressourcenplanung, fehlende Ersatzteile und auch veraltete Übertragungsprotokolle sind auf fehlende Planung und mangelhaftes Projektmanagement zurückzuführen. Nur durch frühzeitige Berücksichtigung der Informationssicherheit und stringentes Planungsmanagement werden informationssicherheitsrelevante Projekte aufgedeckt und können der Kritikalität entsprechend geplant und umgesetzt werden.

7. Ransomware

Ist eine spezielle Art eines hinterhältigen Angriffes bei dem Angreifer die Unternehmensdaten verschlüsseln und Lösegeld verlangen, um die Daten wieder zugänglich zu machen. Manchmal stehlen die Angreifer auch die Daten und verlangen Zahlungen damit die Daten nicht an Behörden, Wettbewerber oder die Öffentlichkeit geschickt werden. Bei den Eintrittstoren für Ransomware stehen Phishing Emails und Remote Desktop Protokoll (RDP) Verbindungen an oberster Stelle.

8. Malware

Malware ist der Überbegriff für Software, Firmware oder Code der in böswilliger Absicht die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen beeinflusst. Zu den Unterformen zählen Viren, Würmer, Trojanische-Pferde, RATs (Remote-Access-Tools) und Code-infektionen von Systemen. Auch zählen manche Spyware und Adware zu Malware. Eine guter Malware-Schutz mit Verhaltensanalyse zur Laufzeit auf allen Systemen (Clients, Server, Gateways) hilft die Infektion und Verbreitung von Malware einzudämmen. Installation von Software und Treiber durch BenutzerInnen auf Endgeräten sollte massiv eingeschränkt sein.

9. Missbrauch bzw. Übernahme von Benutzerkennungen

Beim Missbrauch von Benutzerkennungen bzw. Identitätsdiebstahl täuscht der Angreifer die Identität einer Person vor, um in deren Namen aufzutreten. Dies gelingt besonders einfach, indem man E-Mail Konten hackt und dann über emailbasierte Passwort-Reset Verfahren weitere Dienste übernimmt. Für diese Gefährdung sind starke Passwörter mit zusätzlicher Zwei-Faktor-Authentifizierung der beste Schutz. Gleichzeitig müssen Unternehmen die BenutzerInnen über Security-Awareness Kampagnen bezüglich der Nutzung von einzigartigen Passwörtern und der Gefahr durch Phishing-Angriffe schulen.

10. Cryptojacking

Neu ist die Idee ja nicht Crypto-Mining auf starker Hardware zu betreiben, jedoch wird es zur Straftat, wenn man dabei die Rechenleistung und den Strom eines Opfers nutzt. Hierbei sind gleichermaßen Endgeräte und auch Server betroffen, die von Angreifern infiziert und ausgenutzt werden. Vereinzelt haben auch Softwarehersteller versucht, in ihrer Software und in Plug-Ins entsprechende Mining-Dienste einzubauen und dies mit der kostenfreien Nutzung der Software argumentiert und in einer langen EULA verschleiert.

11. Social-Engineering / Phishing / Spear-Phishing / weitere E-Mail Angriffe

Die Varianz bei Gefährdungen durch Social-Engineering ist groß und inkludiert Pishing, Spear-Phishing, Whailing, Smishing, Vishing und in Zukunft sicher auch Video-Phishing mit Deep-Fake Technologie. Hierbei nimmt das Infektionsmedium E-Mail immer noch die größte Rolle ein. Unternehmen sind angehalten die perfiden Methoden von Social-Engineering Angriffen über aktuelle Beispiele und deren möglichen Auswirkungen in regelmäßigen Security-Awareness Kampagnen und verpflichtenden Schulungen mit allen MitarbeiterInnen zu trainieren.

12. Angriffe auf Daten

Zu den Gefahren durch Angriffe auf Daten zählen unter anderem der unberechtigte Zugriff, unerwünschte Veröffentlichung, falsche Berichtserstattung / Falschinformation, Desinformation (bewusst falsche Informationen zum Zwecke der Täuschung). Oft werden diese Vorfälle als Datenpanne / Data-Breach / Data-Leak bezeichnet und beziehen sich immer auf die Veröffentlichung sensibler, vertraulicher oder geschützter Daten in einer nicht vertrauenswürdigen Umgebung. Besondere Kritikalität entsteht, wenn der Data-Breach personenbezogene Daten gemäß der DSGVO betrifft. Dann muss das Unternehmen diese Datenpanne gegenüber der Behörde anzeigen.

13. Angriff auf die Datenverfügbarkeit inkl. DoS/DDoS

Bei den Angriffen gegen die Datenverfügbarkeit stehen zwei Angriffsmethoden im Vordergrund: Distributed Denial of Service (DDoS) und Angriffe auf Web-Dienste. Ein DoS/DDoS Angriff blockiert kritische IT-Dienste des Unternehmens vollständig, dies können der Internet-Uplink, die E-Mail-Serverdienste, Außenstellenanbindungen oder beliebige andere Dienste wie der Online-Verkauf sein. Bei den Web-basierten Angriffen wird in der Regel die Datenintegrität und Verfügbarkeit adressiert. Hierbei können auch durch manipulierte Web-Links unscheinbare Web-Dienste für die Verteilung von Malware oder für den Diebstahl von Web-Form Daten missbraucht werden.

14. Zielgerichtete Angriffe (APTs)

Der große Unterschied zwischen einem „normalen“ Hacker-Angriff auf eine Infrastruktur und einem Advanced Persistent Threat (APT) ist, dass APT-Angriffe sehr zielgerichtet sind und mit einem hohen Aufwand durchgeführt werden. Hierzu recherchieren die Angreifer teilweise wochenlang die Mitarbeiterverantwortlichkeiten und bestehende Kunden- und Lieferantenbeziehungen bevor der Angriff gestartet wird. Auch wird für einen APT-Angriff oft individuelle Malware entwickelt, die von handelsüblichen Malware-Schutzprogrammen nicht erkannt wird. Oft sind APT-Angriffe primär auf das langfristige Ausspähen der Opfer ausgelegt (Link WIKI: Industrie-Spionage).

15. Angriffe auf SSL Verschlüsselungen

Bei den Angriffen auf SSL Verschlüsselung geht es zum einen um die Gefahr durch selbstsignierte Zertifikate, die einfach per Man-in-the-Middle angegriffen werden können und zum anderen um veraltete, unsichere Kryptographie-Algorithmen und Schlüssellängen die keinen ausreichenden Schutz für Übertragungsprotokolle bieten. Speziell der Einsatz von OpenSSL in Anwendungen und Web-Diensten birgt größere Gefahren, da OpenSSL Verwundbarkeiten (siehe Heartbleed, Poodle) umfassend dokumentiert werden und Angreifer diese unverzüglich auszunutzen versuchen.

16. Angriff auf Web-Anwendungen (OWASP Top 10)

Entwickeln Sie selbst Web-Anwendungen? Dann sollten Sie die 10 wichtigsten Gefahren des Open Web Application Security Project für diesen Anwendungstyp kennen: A1:2021 — Broken Access Control, A2:2021 — Cryptographic Failures, A3:2021 – Injection, A4:2021 — Insecure Design, A5:2021 – Security Misconfiguration, A6:2021 — Vulnerable and Outdated Components, A7:2021 — Identification and Authentication Failures, A8:2021 — Software and Data Integrity Failures, A9:2021 — Security Logging and Monitoring Failures, A10:2021 — Server-Side Request Forgery Leider werden neue oder bestehende Web-Anwendungen nicht regelmäßig auf diese Gefahren untersucht und daher haben es Hacker viel zu leicht Web-Apps zu übernehmen dem Unternehmen zu schaden.

17. Zero-Day Angriffe

Im Prinzip ist eine Zero-Day Verwundbarkeit eine von vielen Schwachstellen, die entdeckt werden, jedoch mit dem Unterschied, dass es für die Schwachstelle noch keinen Patch oder Hotfix gibt. In einer frühen Phase einer Zero-Day Verwundbarkeit liegen oft auch noch keine fundierten Informationen über das Ausmaß und Auswirkung der Schwachstelle vor. Unternehmen sind gefordert solche Zero-Day Verwundbarkeiten frühzeitig zu erkennen, hierzu wird eine zuverlässige Zero-Day Informationsquelle benötigt und eine schnelle Bewertung ob betroffene Dienste im Unternehmen eingesetzt werden.

Klassifizierung: TLP White
Ersteller: Andreas Schuster, SEC4YOU
Version: 1.0
Datum: 8.7.2022

Von Andreas Schuster | 08.07.2022 | Blog, ISMS Tools, Tipps

Über den Autor: Andreas Schuster

Andreas Schuster ist 50 Jahre alt und wohnt in Wien. Vor über 20 Jahren hat er sein Hobby die IT zum Beruf gemacht und arbeitet seit vielen Jahren in der Crypto-Branche. Seit 2015 unterstützt er das SEC4YOU Team. Sein technisches Interesse an allem das ein Kabel hat (exklusive Weißwaren...) bringt immer wieder spannende Blog-Inhalte. Besuchen Sie auch seinen Blog zu Verschlüsselung & IoT unter https://verschlüsselt.IT

Ähnliche Artikel