Resilienz & KRITIS

Warum diese Partnerschaft immer dringlicher wird

Know-how to go Wissensfrühstück 27.04.2022

Marius Wiersch

Marius Wiersch

Marius Wiersch

Managing Consultant & Team Manager

Fachliche Schwerpunkte:

- Kritische Infrastrukturen nach IT-SiG, BSIG und BSI-Kritis-Verordnung
- Beratung zur Informationssicherheit nach ISO 27001 und IT-Grundschutz
- Einführung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 und IT-Grundschutz
- Integration der IDW PS 951 und ISAE 3402 Standards in ISMS

Spezielle Qualifikationen:

- ISO/IEC 27001 Lead Auditor
- Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG
- Auditor für ISO/IEC 27001 EnWG gemäß IT-Sicherheitskatalog nach § 11 Abs. 1a Energiewirtschaftsgesetz
- Auditor für Energieerzeugungsanlagen nach EnWG § 11 Abs. 1b
- BSI IT-Grundschutz-Praktiker
- Foundation Examination TISAX® Assessment

Agenda

1. Kritische Infrastrukturen
2. Bedrohungslage in Deutschland
3. Selbstverteidigung

1. Kritische Infrastrukturen

Regularien in Deutschland

Regulierung für kritische Infrastrukturen begann 2015

Ziel: Kritische Infrastrukturen mit nachgewiesener IT-Sicherheit

Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern

KRITIS und KRITIS im Sinne des BSI-Gesetzes

- KRITIS beschreibt in Deutschland kritische Infrastrukturen, welche für das Gemeinwohl notwendig sind

Kritische Infrastrukturen

Kritische Infrastrukturen sind Anlagen die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind

Kritische Infrastrukturen nach BSI

Einrichtungen, Anlagen die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind.

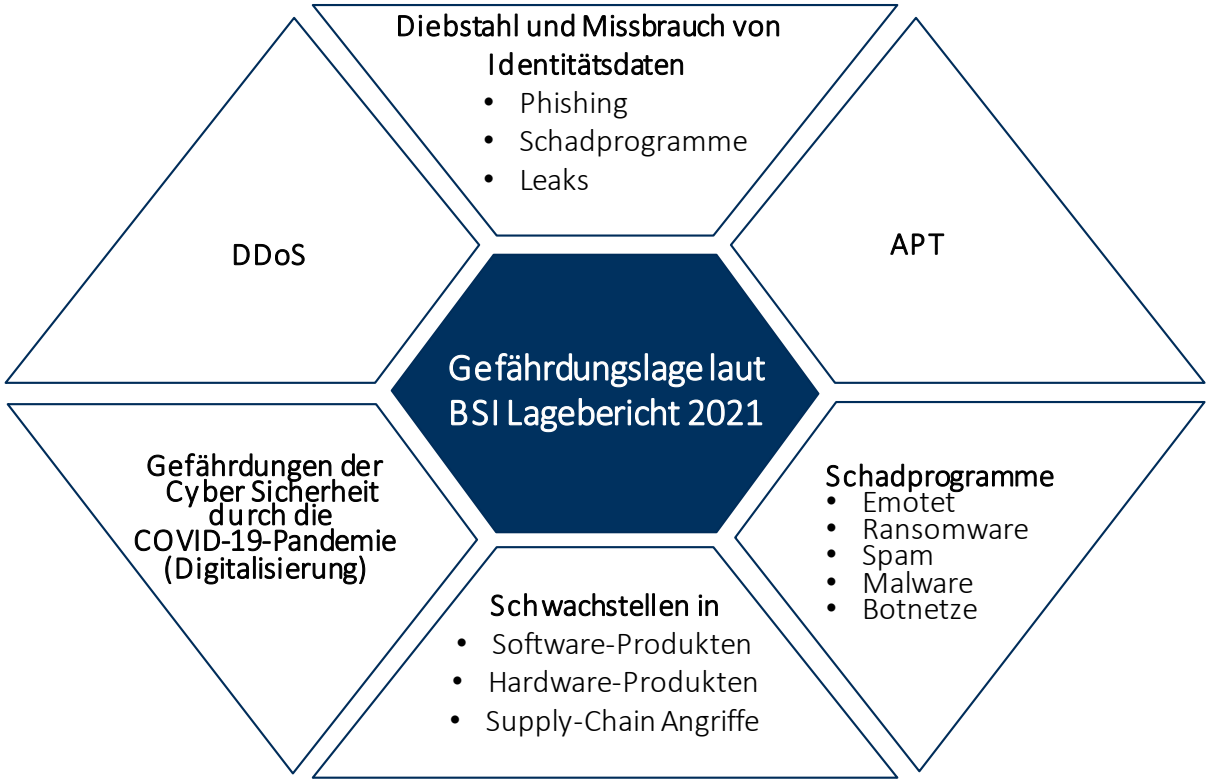
Ob ein bedeutender Versorgungsgrad vorliegt, ist vom Erreichen oder Überschreiten von in der BSI-Kritisverordnung aufgeführten Schwellenwerten abhängig

Kritische IT

IT-Systeme, welche für den Betrieb der kritischen Infrastrukturen nötig sind

2. Bedrohungslage in Deutschland

Die Lage der IT-Sicherheit in Deutschland



Wer greift an

Staatsakteure

- Geopolitische Interessen
- Diebstahl von Wissen

Organisierte Kriminalität

- Phishing
- CEO-Fraud
- Ransomware

Kleinkriminelle

- Abrechnungsbetrug

- Hacking aus Spaß und Neugier
- Erpressung – finanzielle Motivation
- Frust oder Rache – persönliche Motivation
- Ressourcen
- Behinderung von Wettbewerbern
- Betrug – Onlinehandel oder CEO-Fraud
- Spionage

Arten von Angriffen und beispielhafte Methoden

Ungerichtete Angriffe

- Allgemeiner Schadcode
- Phishing-Attacke
- Sniffing-Attacke

Gezielte Angriffe

- Auf das Zielobjekt angepasster Schadcode
- Aufforderung zur Informationsübermittelung
- Man-in-the-Middle-Angriff

Hochprofessionelle Angriffe

- Speziell entwickelter Schadcode
- Ausnutzung von Zero-Day-Exploits

Die Lage der IT-Sicherheit in Deutschland
Quelle: Hiscox Cyber Readiness Report 2020

- Der Median der Kosten für die 1.971 Unternehmen, die von Cyber-Attacken und -Schäden betroffen waren und die die Aufwendungen in den letzten 12 Monaten nachhielten, lag bei 51.200 €. Das ist fast eine Versechsfachung gegenüber den 9.000 € des Vorjahres.
- Die gesamten Cyber-Verluste der betroffenen Unternehmen beliefen sich auf 1,6 Milliarden € im Vorjahr.
- Welche Branchen sind/waren besonders betroffen:
  - Finanzdienstleistungen
  - Produzierendes Gewerbe

Digitalisierung

Im Zuge der Digitalisierung werden immer mehr Informationen digital gespeichert, bearbeitet und verteilt.

Kleinere Unternehmen haben keine großen Ressourcen, müssen aber eine Menge an Daten speichern und verarbeiten.

Mittelständische und große Unternehmen verarbeiten Informationen heute meist vorwiegend digital.

Die steigende Komplexität von Prozessen und Anwendungen führt fast unvermeidbar zu Fehlern in der Entwicklung, Wartung oder Handhabung.

Warum gibt es oft Probleme

Die IT wächst ohne Struktur.

Oft kommt günstige Hard- und Software zum Einsatz.

Externe Anforderungen fordern mehr Einsatz von IT (Ausschreibungen, Bestellungen, Kommunikation).

Meist macht jemand die IT „mit“.

Man investiert in Hardware/Software-Lösungen statt in Wissen.

Folgen der Nicht-KRITIS Angriffe

Betroffene sind „nur“ Mitarbeiter oder Business-Kunden.

Sind Endkunden betroffen, gibt es Alternativen am Markt.

Der Schaden ist in der Regel zum Schluss „nur“ finanziell.

Warum sind KRITIS anders

KRITIS-Bewusstsein fehlt oft:
Safety vs. Security

KRITIS müssen mehr digitalisieren.

KRITIS sind da wo man sie braucht.

Warum sind KRITIS anders

KRITIS sind für die Region alternativlos.

Warum ist KRITIS anders

Ausfall von KRITIS führt schnell zu sozialen Unruhen.

3. Selbstverteidigung

Grundsätzlich: Die beste Verteidigung ist nicht angegriffen zu werden!

Einfallstore absichern und abschrecken durch Vorbereitung, denn es wird nach einfachen Opfern gesucht.

Problem: Als Kritische Infrastruktur sollte man davon ausgehen angegriffen zu werden (wenn man es nicht schon wurde und nicht bemerkte).

Hier hilft nur die Resilienz zu erhöhen, um im aktiven Angriffsfall trotzdem zu funktionieren.

Übersicht an Maßnahmen

- Mitarbeitersensibilisierung
- Identitäts- und Berechtigungsmanagement
- Multi-Faktor-Authentisierung (MFA)
- Passwortmanager
- Detektion und Reaktion
- Absicherung des Unternehmensnetzwerks
- Zeitnahes Patchen
- Absicherung der Clients und Sever
- Datensicherung
- Vorbereitung auf Sicherheitsvorfall
- Notfallmanagement

Folgekosten eines Vorfalls betragen ein vielfaches der Investitionen in Präventationsmaßnahmen.

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch offene Fragen zum Thema Resilienz?