solutionIT

#ITkluggesichert

„Aufbau einer IT-Sicherheitsstrategie für mein Unternehmen“

Olaf Otahal

solutionIT GmbH

AKITK

Lübeck, 02.07.2025

IHK Lübeck

Wer sind wir und was machen wir?

solutionIT GmbH aus Bad Oldesloe ist ein Anbieter und Dienstleister von maßgeschneiderten IT-Sicherheitslösungen für Unternehmen aller Größen und Branchen. Mit unserem fundierten Fachwissen und unserer langjährigen Erfahrung unterstützen wir Unternehmen dabei, ihre IT-Infrastrukturen und digitalen Assets zu schützen, Bedrohungen zu erkennen und darauf zu reagieren, sowie sich erfolgreich gegen die ständig wachsenden Bedrohungen aus dem Cyberspace zu verteidigen.

solutionIT

solutionIT

Aktuelle Bedrohungslage

#ITkluggesichert

Top 3-Bedrohungen je Zielgruppe

#ITkluggesichert

Gesellschaft

Identitätsdiebstahl

Erpressung

Fake-Shops im Internet

Wirtschaft

Ransomware

Schwachstellen, offene oder falsch konfigurierte Online-Server

IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat & Verwaltung

Ransomware

Schwachstellen, offene oder falsch konfigurierte Online-Server

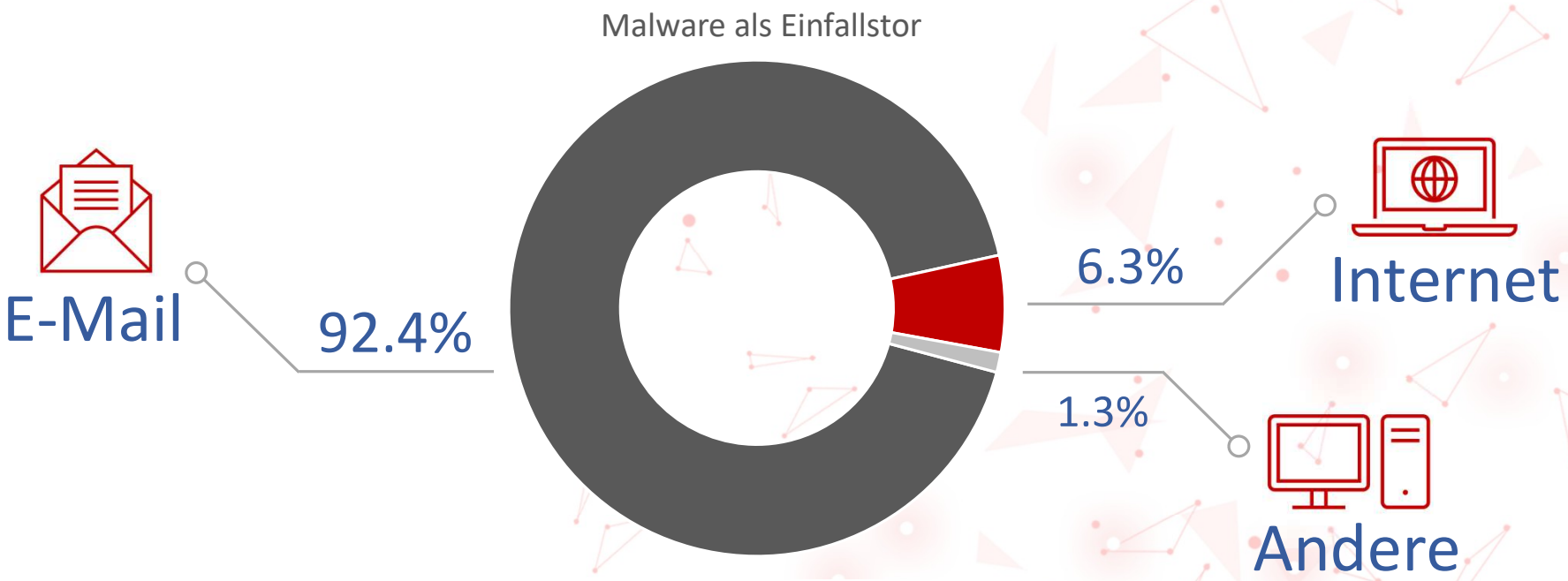
APT

Quelle: BSI

solutionIT

Einfallstore durch Malware

#ITkluggesichert



Quelle: Online Finances

solutionIT

Lage der IT-Sicherheit in Deutschland in 2024

#ITkluggesichert

15 Millionen

Meldungen zu Schadprogramm-Infektionen in Deutschland, übermittelte das BSI an deutsche Netzbetreiber.

207 Tage

Erster digitaler Katastrophenfall in Deutschland

-> LK Anhalt-Bitterfeld

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

117 Millionen zugenommen.

69% aller Spam-Mails waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

Quelle: BSI - https://www.bsi.bund.de/

solutionIT

Aktuelle Bedrohungsbeispiele

#ITkluggesichert

Lagebild 2024

Hohe Bedrohungslage durch Cyberkriminalität

Stand: 03.06.2025 15:38 Uhr

Deutschland steht im Fokus von Cyberkriminellen: Laut dem Lagebild Cybercrime liegt die Bedrohung auf hohem Niveau, die Angriffe aus dem Ausland nehmen weiter zu. Innenminister Dobrindt will im Kampf gegen Cyberattacken massiv aufrüsten.

Quelle: https://www.tagesschau.de/

Bundeslagebild Cybercrime 2024

Bedrohungslage in Deutschland ist anhaltend hoch

04.06.2025 · Von Melanie Staudacher · 3 min Lesedauer ·

Geopolitische Entwicklungen, Künstliche Intelligenz sowie internationale Cyberoperationen haben das IT-Security-Jahr 2024 geprägt. Darauf geht das Bundeskriminalamt in seinem Bundeslagebild Cybercrime 2024 ein und positioniert sich als mögliche zentrale Stelle für die Bekämpfung von Cyberkriminalität.

Quelle: https://www.security-insider.de/

FASANA

Ransomware-Angriff am 19. Mai 2025

Ransomware

Fasana stellt Insolvenzantrag nach Cyberangriff

24.06.2025 · Von Melanie Staudacher · 2 min Lesedauer ·

Der Serviettenhersteller Fasana erlitt einen Ransomware-Angriff. Weil daraufhin nicht mehr produziert werden konnte, meldete das Unternehmen Insolvenz an. Fasana sucht nun nach einem Käufer, damit die rund 240 Stellen gerettet werden können.

Quelle: https://www.security-insider.de/

Es ist nicht die Frage, ob es passiert, sondern wann es passiert!

solutionIT

„Aufbau einer IT-Sicherheitsstrategie für mein Unternehmen“

Praxisnaher Leitfaden für Entscheider und IT-Verantwortliche, keine Hersteller oder Produkt Präsentation

#ITkluggesichert

Zielsetzung

- Entwickeln Sie ein Verständnis für den Aufbau und die Notwendigkeit einer IT-Sicherheitsstrategie
- Steigende Cyberbedrohungen und neue Vorschriften sorgen für den richtigen Moment, um hier ein Projekt zu starten

solutionIT

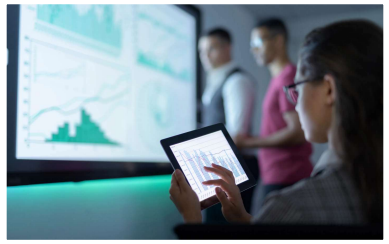
Herausforderungen

➞ Technologien

- unzählige punktuelle Produkte
- Best-of-Breed-Ansatz
- häufige False-Positives

➞ Menschen

- hohe Fluktuationsrate
- wiederholende langweilige Aufgaben
- keine Zeit für Projekte oder Entfaltung



➞ Geld

- teure und komplizierte Lösungen mit hoher TCO
- Kosten sprengen die Budgets

solutionIT

Was ist eine IT-Sicherheitsstrategie?

- Langfristiger Plan zur Absicherung Ihrer IT-Infrastruktur
- Bestandteile sind: Schutz, Erkennung, Reaktion und Wiederherstellung
- Wichtig: Verknüpfung mit der Unternehmensstrategie

solutionIT

6 Schritte zu einer IT-Sicherheitsstrategie

#ITkluggesichert

1. Ist-Analyse
2. Zieldefinition
3. Risikoanalyse
4. Maßnahmenplan
5. Umsetzung & Schulung
6. Monitoring & Verbesserung

solutionIT

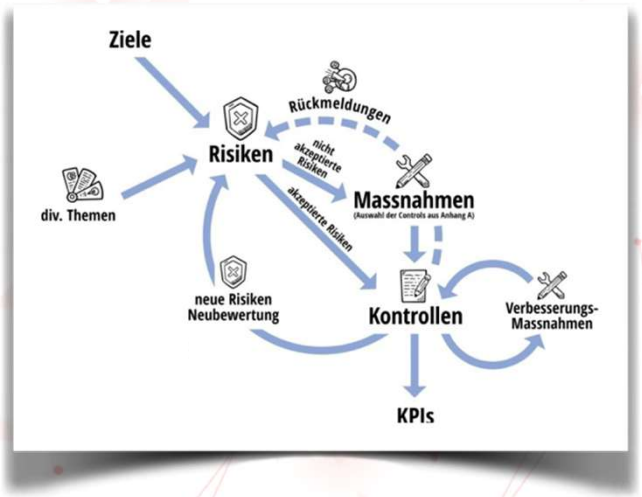
Schritt 1 - die Ist-Analyse

- Systeme, Prozesse & Datenflüsse identifizieren und dokumentieren
- Schwachstellen identifizieren
- Compliance prüfen, z. B. DSGVO, NIS2, DORA, KRITIS

solutionIT

Schritt 2 - Festlegung der Ziele & Prioritäten

- Schutzbedarf definieren
- Kritische Prozesse priorisieren
- Ziele geschäftlich verankern



solutionIT

Schritt 3 - die Risikoanalyse

- Bedrohung bewerten
- Risiko = Eintrittswahrscheinlichkeit * Schadensausmaß
- eine Risikostrategie daraus ableiten

solutionIT

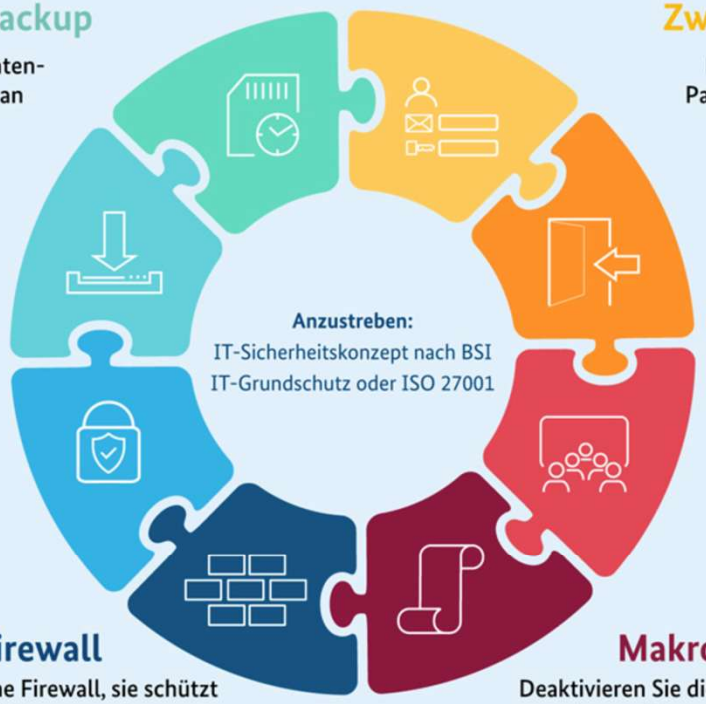
Schritt 4 - der Maßnahmenplan (TOMs)

- Technische Maßnahmen
  - Perimeter Firewall und Segmentierungs-Firewall
  - Endpoint Security möglichst mit EDR Erweiterung
  - …
- Organisatorische Maßnahmen
  - Richtlinien, z.B. für Passwörter, Umgang mit mobilen Geräten
  - Prozesse, z.B. Löschvorgaben, On- und Offboarding
  - …
- eine Notfall- und Wiederherstellungsplanung

solutionIT

Basiselemente der Cyber-Sicherheit

– insbesondere für Kleinst- und Kleinunternehmen –



Datensicherung/Backup

Legen Sie regelmäßig Datensicherungen/Backups an

Zwei-Faktor Authentisierung

Neben dem ersten Faktor, meist einem Passwort, nutzen Sie einen zweiten Faktor, z.B. Push-TAN oder Personalausweis

Updates

Halten Sie Ihre Software durch Sicherheits-Updates auf dem neuesten Stand

Passwörter

Verwenden Sie möglichst starke und unterschiedliche Passwörter. Nutzen Sie idealerweise einen Passwortmanager

Virenschutz

Überprüfen Sie Ihre gesamte IT auf Anzeichen einer Infektion

Schulen und Sensibilisieren

Informieren Sie regelmäßig über die korrekte Nutzung der zur Verfügung gestellten IT und die Gefahren der Nutzung

Firewall

Nutzen Sie eine Firewall, sie schützt vor Angriffen von außen

Makros abschalten

Deaktivieren Sie die Ausführung von Makros oder lassen Sie nur freigegebene Makros zu

Quelle: Bundesamt für Sicherheit in der Informationstechnik

solutionIT

Schritt 5 - Umsetzung und Awareness

- Realistische Projektplanung und konsequente Umsetzung
- Regelmäßige Schulung der Mitarbeiter*innen
- die Sicherheitskultur regelmäßig stärken

solutionIT

Schritt 6 - Monitoring & Verbesserung

- Infrastruktur Monitoring, LogManagement, E/MDR, SIEM, mSOC, Penetrationtests
- Regelmäßige Audits und Reviews
- die Strategie regelmäßig anpassen

solutionIT

Integration ins Unternehmen

#ITkluggesichert

- Sicherheit als Führungsaufgabe
- Zusammenarbeit der Fachabteilungen mit der IT
- zukünftige Budgets sichern
- externe Beratung nutzen

→ Entwickeln Sie ein Verständnis für den Aufbau und die Notwendigkeit einer IT-Sicherheitsstrategie

solutionIT

Next Steps

- ✴ erste Maßnahmen identifizieren
- ✴ Verantwortlichkeiten festlegen
- ✴ Strategieentwicklung starten

→ Steigende Cyberbedrohungen und neue Vorschriften sorgen für den richtigen Moment, um hier ein Projekt zu starten

solutionIT


Haben Sie Fragen?
Besuchen Sie uns
auf Stand #20
solutionIT