Wo operative auf organisatorische Sicherheit trifft

Dr. Patrick Kühtreiber, Infotech

Warum brauchen wir organisatorische Sicherheit (ISMS)?

Das produziert nur unnötig Papier…

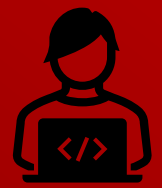
Informationssicherheit schränkt nur ein…

Wir haben eh Backups…

Wir haben eh eine Firewall…



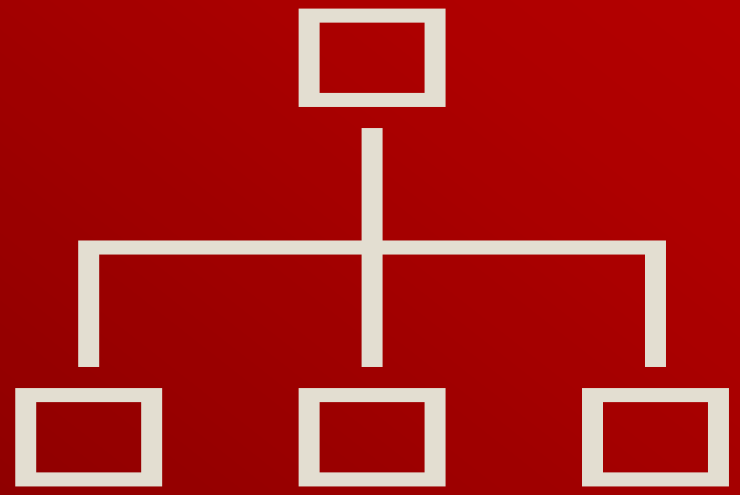
Der Vorfall



```
'; UPDATE users SET password='' WHERE user='admin'--
```

Schritt 1
Kompromittierung eines Systems

Angreifer wird Administrator auf dem System



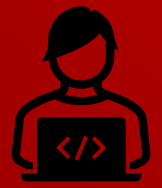
Veraltete Wordpress-Version mit bekannter SQL-Injection Schwachstelle

Der Vorfall

Schritt 2
Kompromittierung des Webservers

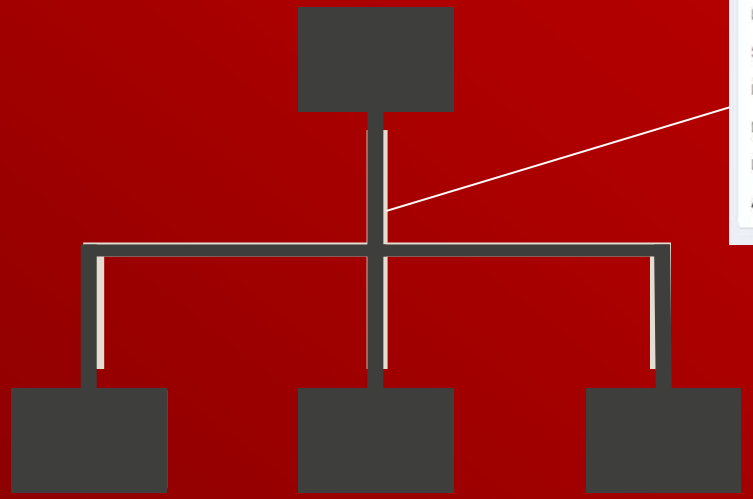
Zero-Day bei Webhosting Software

Kompromittierung am 27.07.2026



Angreifer übernimmt den gesamten Webserver

Angreifer hat Zugriff auf alle Systeme auf dem Server

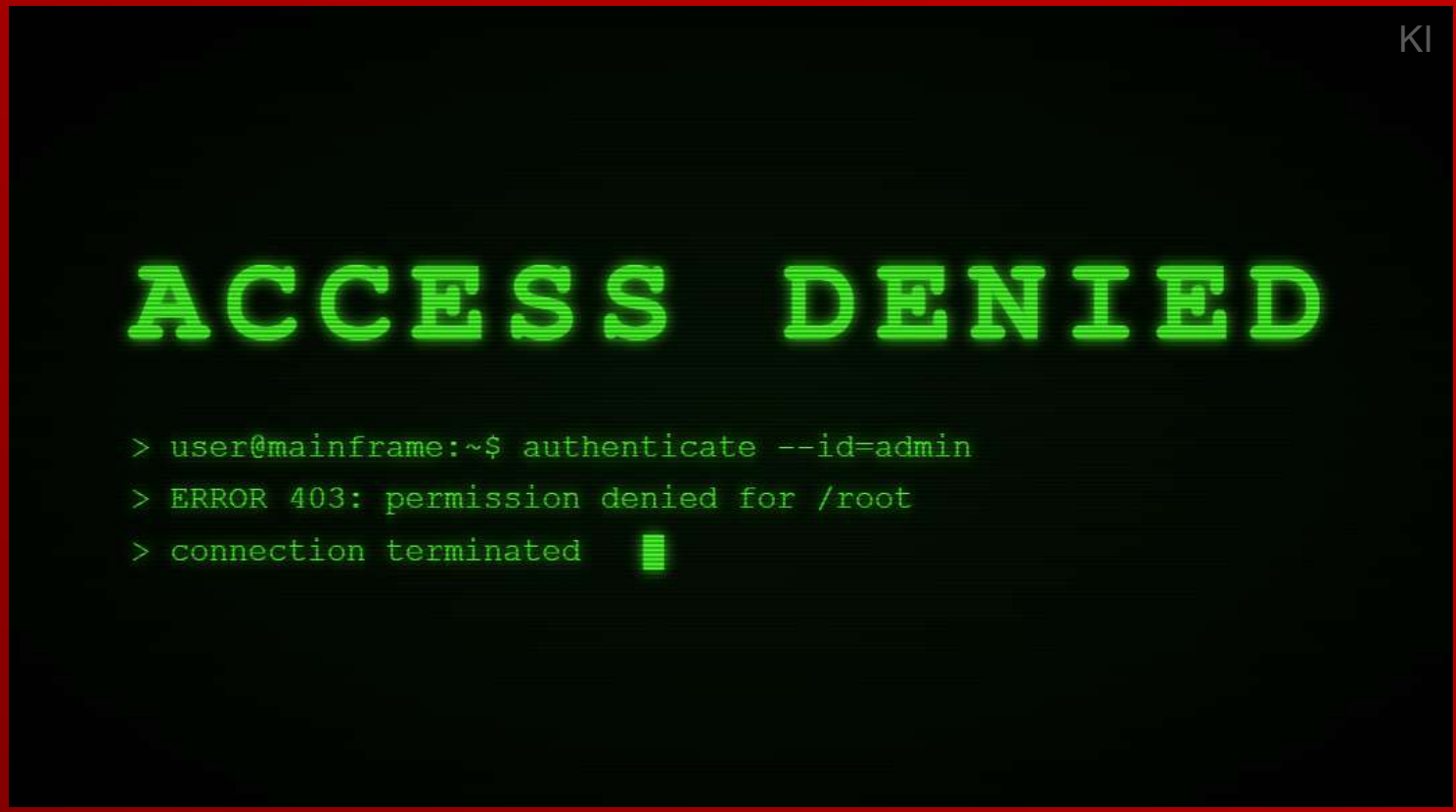




Der Vorfall

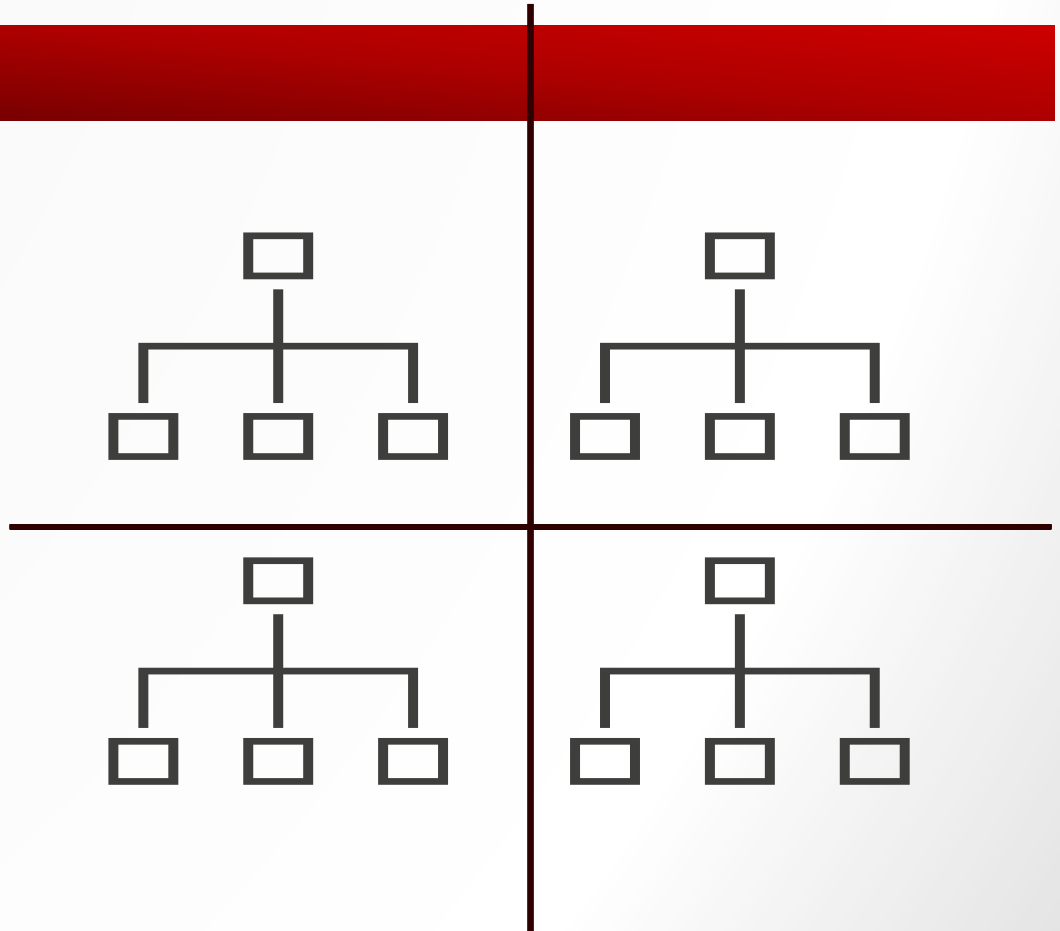
Schritt 3
Angreifer ändert alle Passwörter

Kein Zugriff mehr auf alle Systeme



Maßnahme

Netzwerksegmentierung

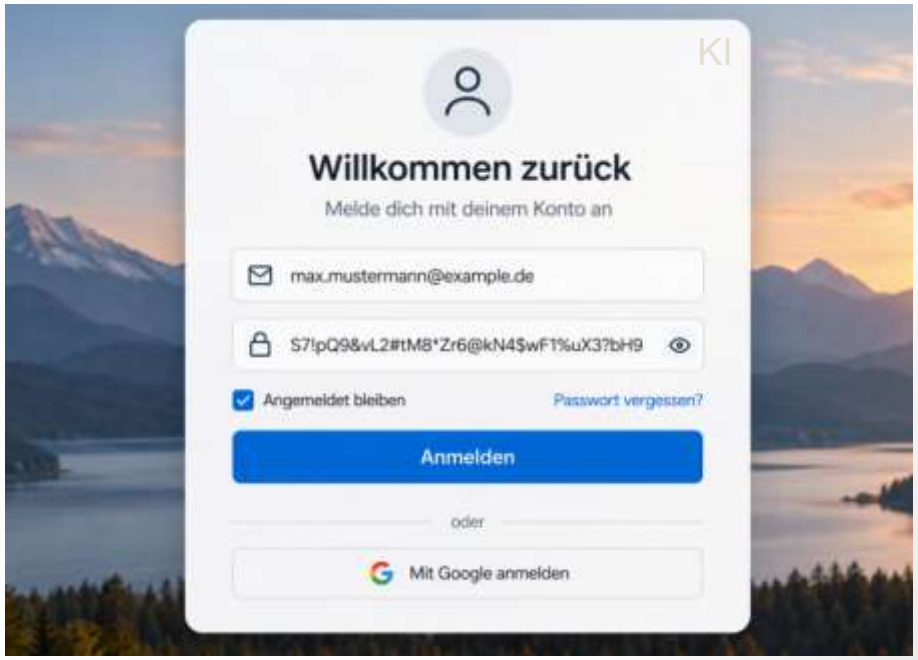


Wie uns das ISMS geholfen hat

Maßnahme

Netzwerksegmentierung

Passwort-Policy



Wie uns das ISMS geholfen hat

Maßnahme

Netzwerksegmentierung

Passwort-Policy

Backup



Wie uns das ISMS geholfen hat

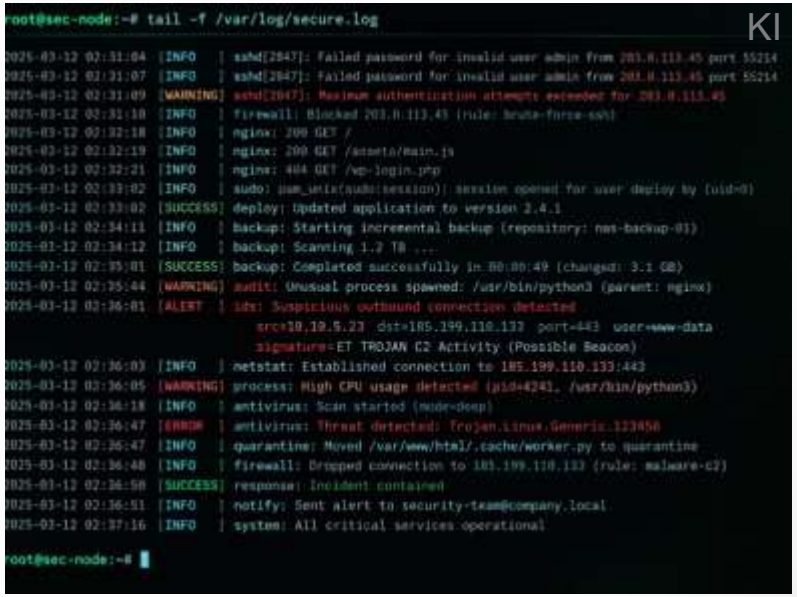
Maßnahme

Netzwerksegmentierung

Passwort-Policy

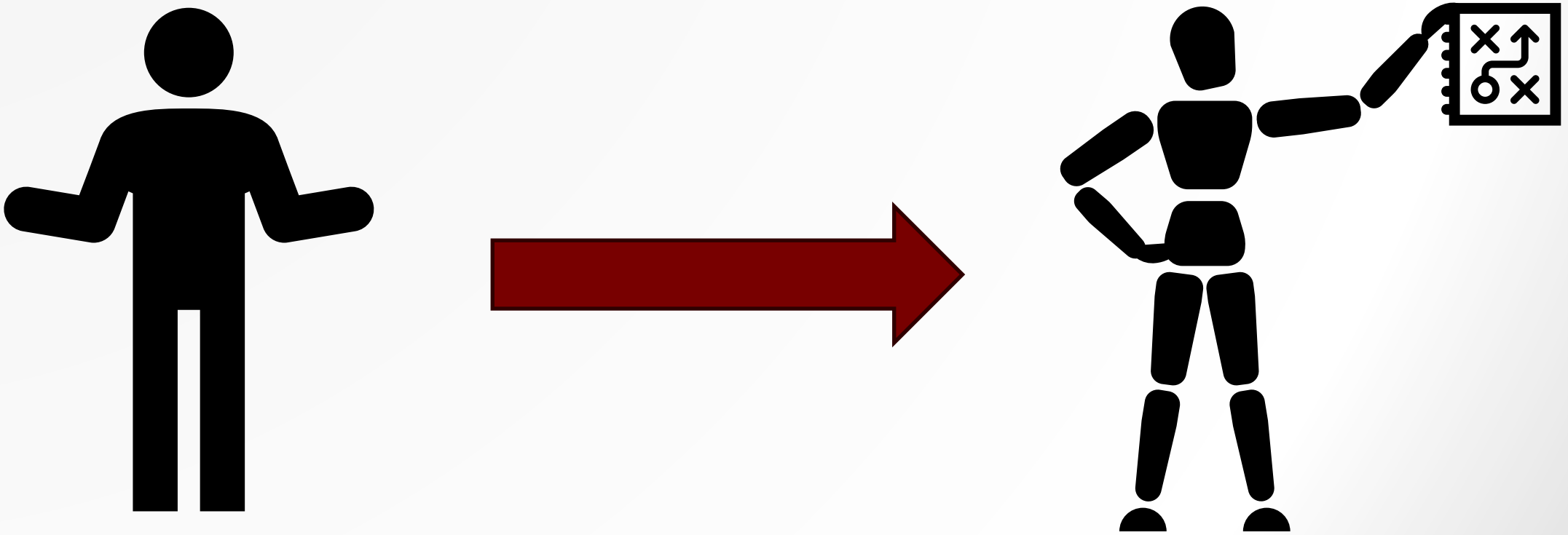
Backup

Logs




There is no
silver bullet
KI

Wenn trotzdem etwas passiert?



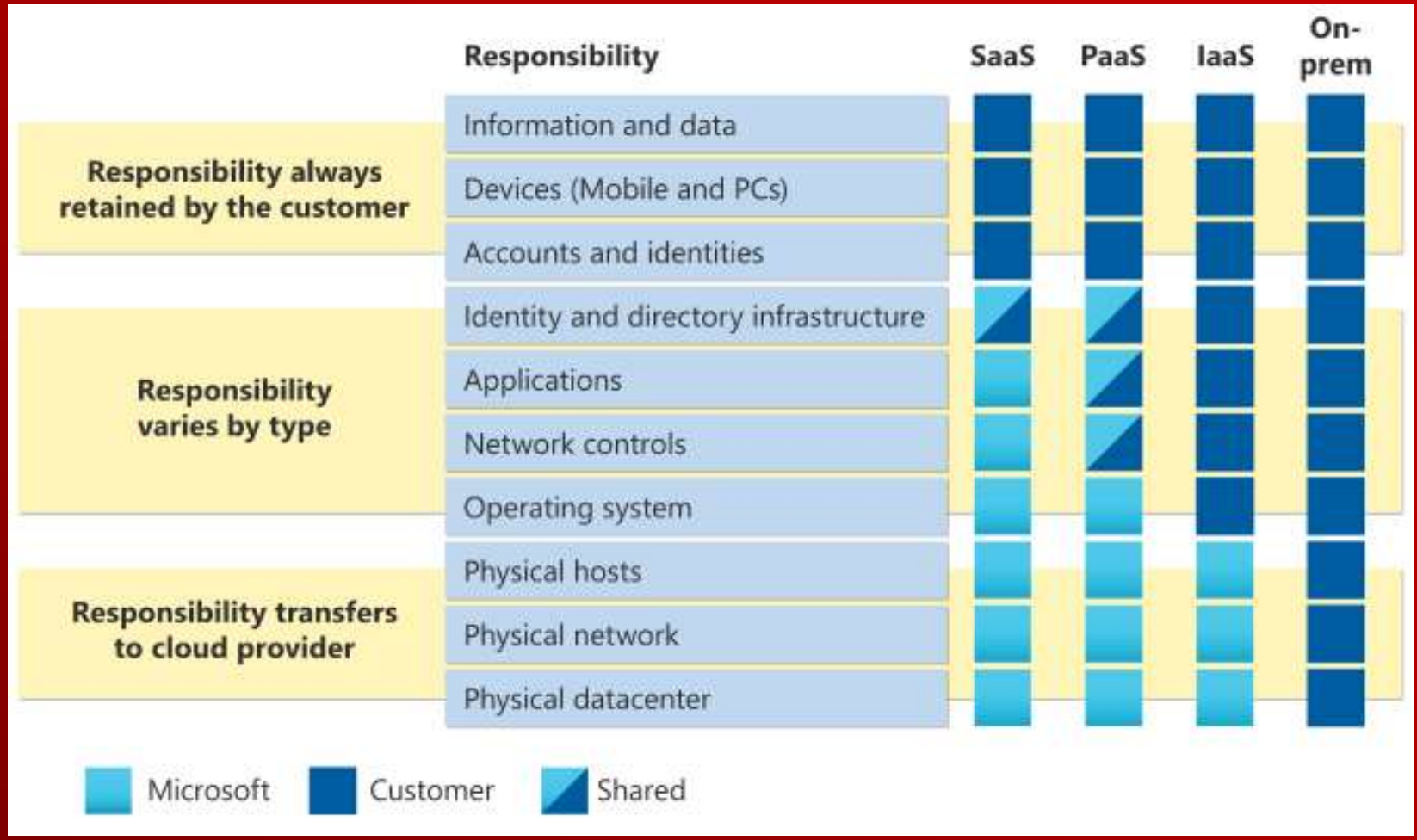
Backups

Klassifizierung je System und gesetzlicher Anforderungen

Backups

Klassifizierung je System und gesetzlicher Anforderungen

Beispiel: O365 Backup



Notfallpläne

Szenario-spezifsiche Sofortmaßnahmen für kritische Geschäftsprozesse

Meldewege

Gesetzliche Meldepflichten vorbereiten

Meldewege

Gesetzliche Meldepflichten vorbereiten

Beispiele für NIS2-Meldungen

Anhang 2

Bewertung der Meldepflicht von Informationssicherheitsvorfällen

Ist bei einem oder mehreren der folgenden Punkte die Antwort „Ja“, so ist der Vorfall der nationalen Cybersicherheits-Behörde zu melden:

DNS:

- Ein rekursiver oder autoritativer Dienst zur Auflösung von Domainnamen ist mehr als 30 Minuten vollständig nicht verfügbar
- Ein rekursiver oder autoritativer Dienst zur Auflösung von Domainnamen benötigt über den Zeitraum von mehr als einer Stunde mehr als 10 Sekunden für eine Antwort
- Die Integrität, Vertraulichkeit oder Authentizität von mindestens 18 Domainnamen ist beeinträchtigt

Übungen

Wir sind vorbereitet

ISMS schafft Sicherheit

Überblick über die Bedrohungslage

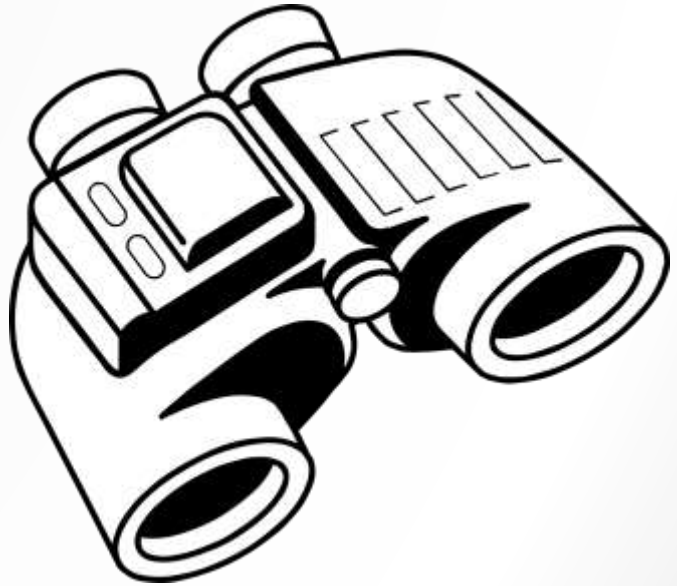


Trends basierend auf bei der Polizei eingelangten Anzeigen

ISMS schafft Sicherheit

Überblick über die Bedrohungslage

Gesamtheitlicher Blick über das gesamte Unternehmen

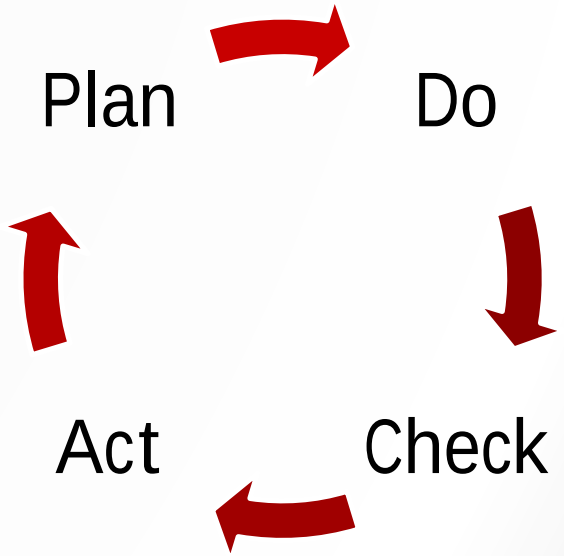


ISMS schafft Sicherheit

Überblick über die Bedrohungslage

Gesamtheitlicher Blick über das gesamte Unternehmen

Lessons Learned und kontinuierlicher Verbesserungsprozess



ISMS schafft Sicherheit

Überblick über die Bedrohungslage

Gesamtheitlicher Blick über das gesamte Unternehmen

Lessons Learned und kontinuierlicher Verbesserungsprozess

Wenn ISMS, Risikomanagement und BCM zusammengreifen, können auch Notfälle und Krisen bewältigt werden


SECURITY IS A
PROCESS, NOT A
PRODUCT

Vorgehensweise

- Pragmatisch
- Lösungsorientiert
- Kontinuierlich



Was soll erreicht werden? Was ist das Ziel?



IST-Stand erheben (GAP-Analyse)



Umsetzen der Maßnahmen



Aufrechterhaltung des Sicherheitsniveaus