



Herzlich willkommen
beim Bundesamt für Cybersicherheit



Cybersicherheit ist Chefsache: Sicherheit und Risikomanagement

Florian Schütz, Direktor Bundesamt für Cybersicherheit

Swissbau - 19. Januar 2024



Inhalt

- Das Nationale Zentrum für Cybersicherheit NCSC
- Aktuelle Lage
- Grundlagen zur Cybersicherheit
- Cybersicherheit ist Chefsache



Bundesamt für Cybersicherheit BACS

Auftrag: Unterstützung der Öffentlichkeit beim Schutz vor Cyberrisiken.

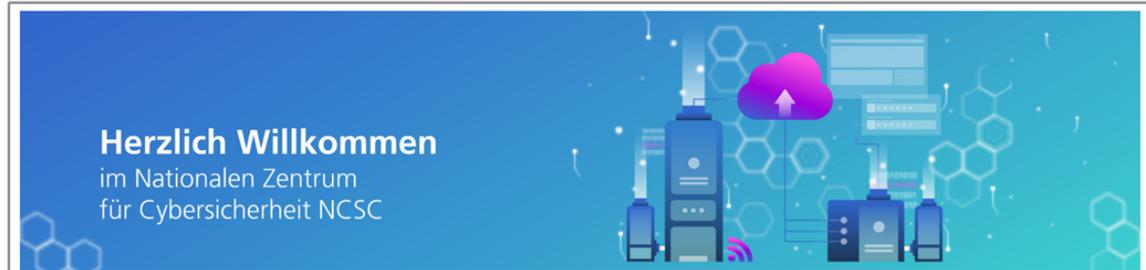
Nationale Cyberstrategie (NCS)



NCS: Grundlage zur Umsetzung der Massnahmen zum Schutz der Schweiz vor Cyberrisiken

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat



Herzlich Willkommen
im Nationalen Zentrum
für Cybersicherheit NCSC

Informationen für

-  Privatpersonen
-  Unternehmen
-  Behörden
-  IT-Spezialisten

Melden Sie uns

-  einen Cybervorfall
-  eine Schwachstelle

Rechtliche Grundlage: ISG/ISV

Leistungen des NCSC

- Cyberbedrohungen verständlich machen
- Mittel zur Verfügung stellen, damit Angriffe verhindert werden können
- Schäden aus Cybervorfällen reduzieren
- Sicherheit von digitalen Produkten und Dienstleistungen erhöhen



Relevante Angebote im Rahmen der NCS

- Cyber-Safe: «erschwingliches» Audit, Standortbestimmung
- Cyber Seal: zertifizierte IT-Dienstleister
- Cybero (ehem. KMU-Schnelltest): Standortbestimmung
- Leitfaden KMU
- Fragen Sie uns!





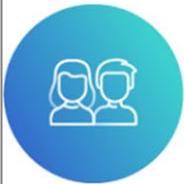
Webseite NCSC

Herzlich Willkommen

im Nationalen Zentrum
für Cybersicherheit NCSC



Informationen für



Privatpersonen Unternehmen



Behörden



IT-
Spezialisten

Melden Sie uns



einen
Cybervorfall



eine
Schwachstelle

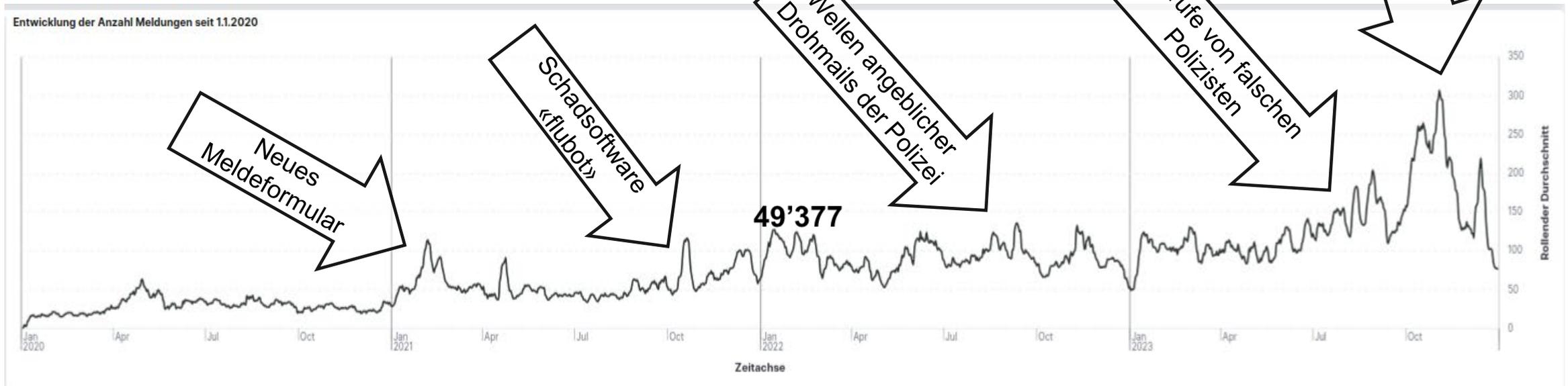


Inhalt

- Das Nationale Zentrum für Cybersicherheit NCSC
- Aktuelle Lage
- Grundlagen zur Cybersicherheit
- Cybersicherheit ist Chefsache



Anzahl Meldungen 2020 – 2023



2020
10833 Meldungen

2021
21714 Meldungen

2022
34527 Meldungen

2023
49377 Meldungen



Was wird gemeldet?

Meldungen 2022

Total: 34'527

20950 Betrug
4487 Phishing
460 Hacking
410 Malware (159 Ransomware)
39 Datenabfluss

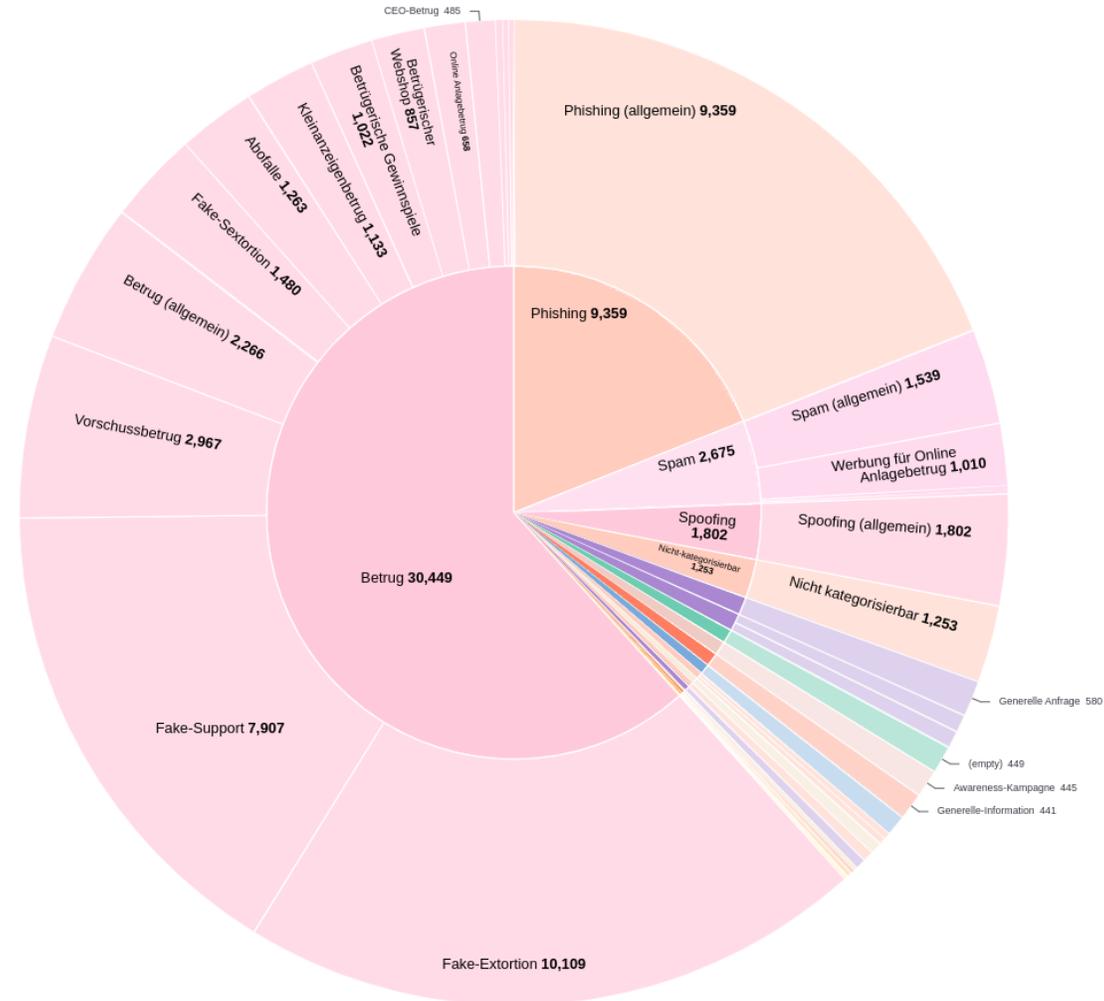
Meldungen 2023

Total: 49'377

30449 Betrug
9359 Phishing
567 Hacking
215 Malware (109 Ransomware)
44 Datenabfluss



Was wird gemeldet?





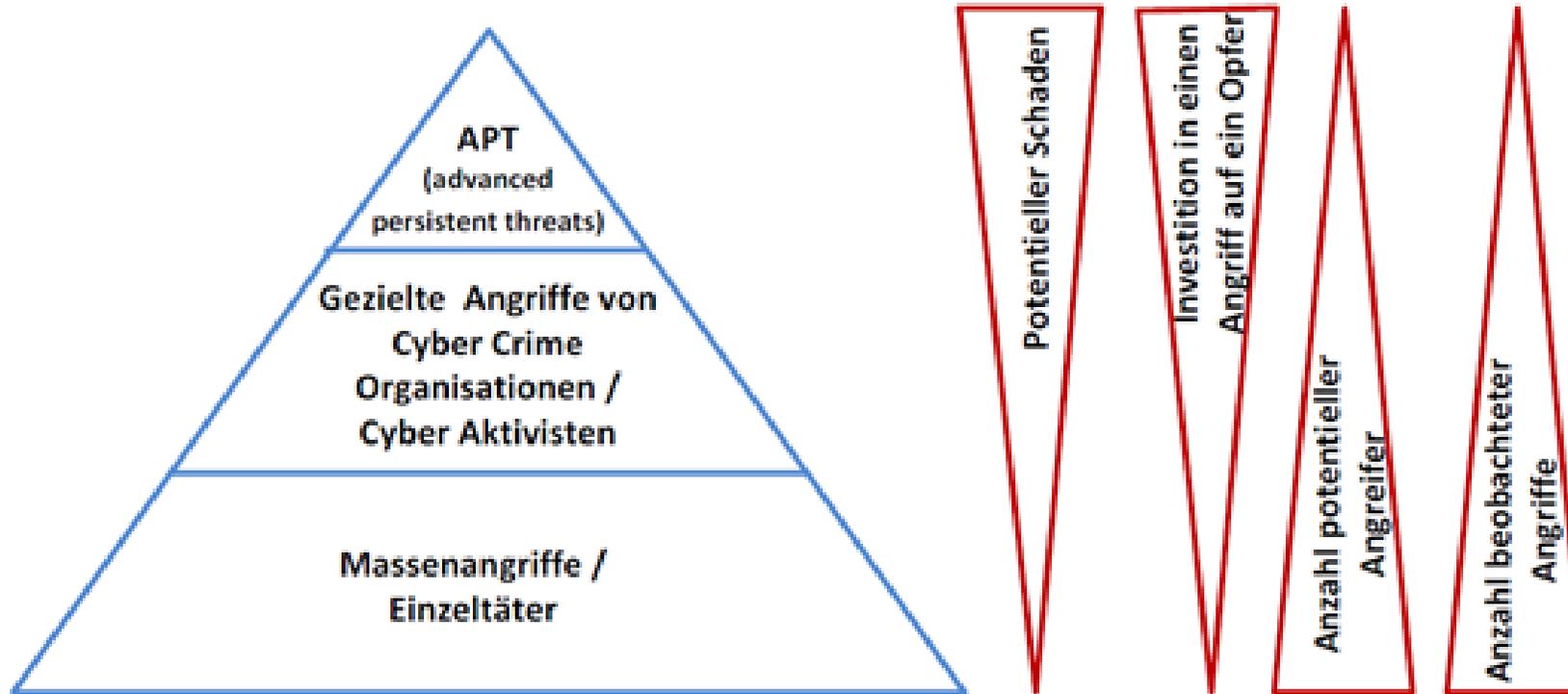
Inhalt

- Das Nationale Zentrum für Cybersicherheit NCSC
- Aktuelle Lage
- Grundlagen zur Cybersicherheit
- Cybersicherheit ist Chefsache



Akteure hinter Cyberangriffen

Bedrohungen für die Unternehmen

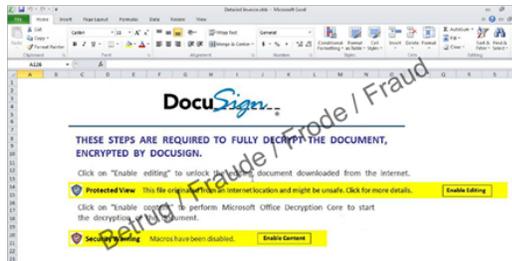


Bedrohungspyramide, adaptiert nach sans.org



Infektionsvektoren: Zwei Hauptwege

Über Mitarbeitende



Über schlecht administrierte und nicht gepatchte Systeme

MS Exchange-Lücken werden noch immer nicht geschlossen

16.05.2022 - Erneut hat das NCSC über 200 Unternehmen mittels eingeschriebenem Brief über verwundbare Microsoft Exchange-Server informiert und gewarnt. Die Sicherheitslücken sind seit Langem bekannt und werden von Cyberkriminellen aktiv ausgenutzt.



Extortion Economics

Ransomware's new business model

Cyber Signals
August 2022

80%

Over 80 percent of ransomware attacks can be traced to common configuration errors in software and devices.

Quelle: Cyber Signals / Microsoft



CEO Betrug – Low Tech mit grossem Erfolg und grossem finanziellem Schaden

Liebe Veronica

Ich bin gerade an einer Tagung und du müsstest mir einen Gefallen tun. An der Veranstaltung X habe ich mich mit Thomas Muster geeinigt, ein gemeinsames Projekt zu starten. Alles ist noch sehr geheim, ich bitte um Vertraulichkeit. Um das Projekt zu initiieren, bitte ich dich, die folgende Zahlung möglichst umgehend auf folgendes Konto zu überweisen:

CHF 50'000.00 an die IBAN: AL023569854125632, Verwendungszweck: Projekt, vertraulich

Ich kann gerade nicht telefonieren, melde mich per Mail.

Liebe Grüsse,
Roger

Geheimhaltung, Druck

Grosse Summe auf unbekanntes Konto

Person angeblich nicht via alternativen Kanal erreichbar

Funktionen, Namen, E-Mail-Adressen finden die Betrüger auf der Firmenwebseite



Business E-Mail Compromise – der grosse Bruder des CEO-Betrugs





Ransomware: hohes Schadenspotenzial



News

Xplain: Hackerangriff hat Folgen

Veröffentlichung: 04.10.2023, 17:02 Uhr • 1 Minute • 0

Bei einem Angriff auf die Software-Firma Xplain im Frühling erbeuteten Hacker mehrere hundert Gigabyte Daten. Darunter auch geheime Dokumente des Bundes. Der Angriff zeigt die Abhängigkeit des Bundes von privaten Firmen.

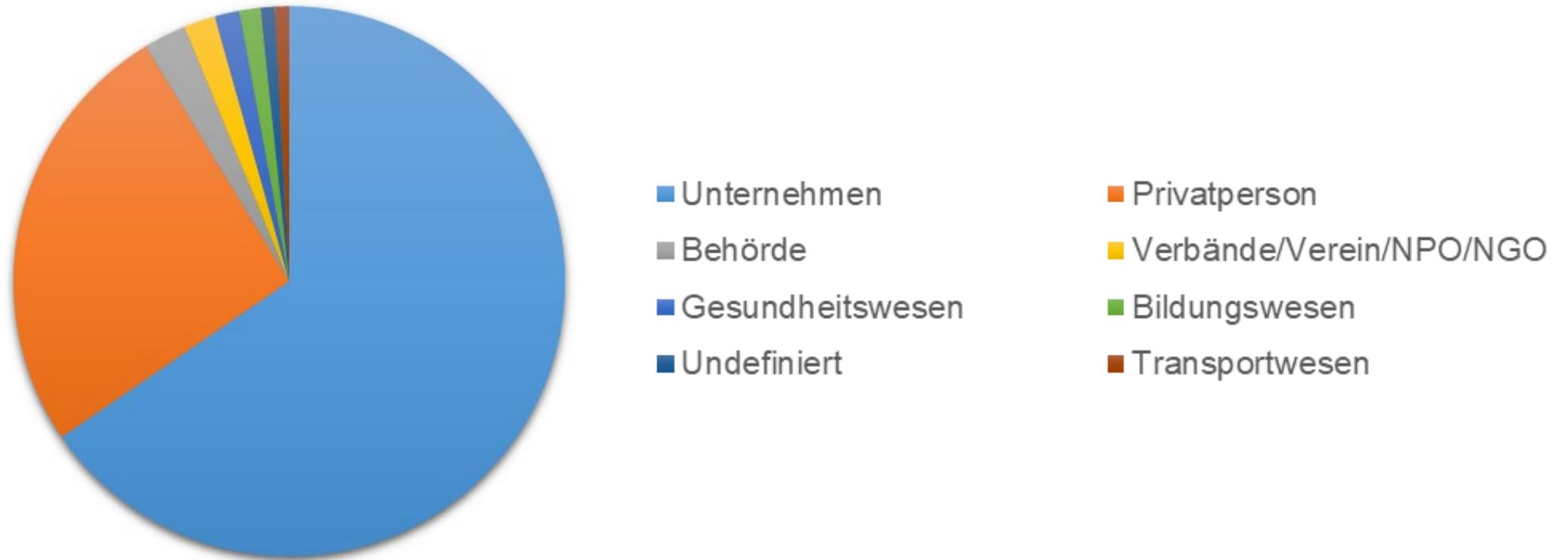
Die Fremdenpolizei der Stadt Bern kann etwa eine App nicht mehr nutzen, mit welcher die Mitarbeitenden bei Kontrollen Fingerabdrücke vor Ort nehmen und sehen, ob eine Person zur Fahndung ausgeschrieben ist. Dies zeigen Recherchen von SRF Investigativ.

Alleine der Bund hatte in den vergangenen vierzehn Jahren Softwarelösungen und Dienstleistungen im Wert von über 32 Millionen Franken bei Xplain beschafft.

Quelle:swisstxt



Ransomware: betroffene Sektoren 2020-2023





Inhalt

- Das Nationale Zentrum für Cybersicherheit NCSC
- Aktuelle Lage
- Grundlagen zur Cybersicherheit
- Cybersicherheit ist Chefsache



Mögliche Folgen eines Cybervorfalls

- Verschlüsselung/Diebstahl von Daten
- Ausfall Webseite/IT-Infrastruktur
- Finanzielle Einbussen (Umsatzeinbrüche, Schadenersatzklagen)
- Reputationsschaden



Individuelle Risiken und Kosten

- Was kostet mein Unternehmen ein Tag ohne funktionierende Webseite oder IT-Infrastruktur?
- Was kostet mein Unternehmen der Verlust der Hälfte seiner Kundschaft, wenn deren Daten an Dritte gelangen (Vertrauensverlust)?
- Inwiefern haftet mein Unternehmen für gestohlene Kundendaten?
- Was kostet mein Unternehmen der Verlust/die Veröffentlichung von vertraulichen Daten?



Ein Beispiel: Projektwettbewerb I

Sie sind Planerin oder Architekt und nehmen an einem Projektwettbewerb teil. Sie haben eine Deadline zur Einreichung Ihres Projekts.

Sie werden Opfer eines Angriffs, Ihre Projektdaten werden verschlüsselt und Sie werden erpresst. Bezahlen Sie nicht, drohen die Angreifer mit der Veröffentlichung der Daten.



Ein Beispiel: Projektwettbewerb II

Sie reagieren richtig und trennen Ihre Computer vom Netz. Sie haben ein funktionierendes Backup, aber es braucht 2 Tage, um es einzuspielen und das System wieder zum Laufen zu bringen.

Sie bezahlen nicht. Ihre Projektdaten werden im Internet, sichtbar für Ihre Konkurrenten, veröffentlicht.

Der Vorfall gelangt an die Medien.

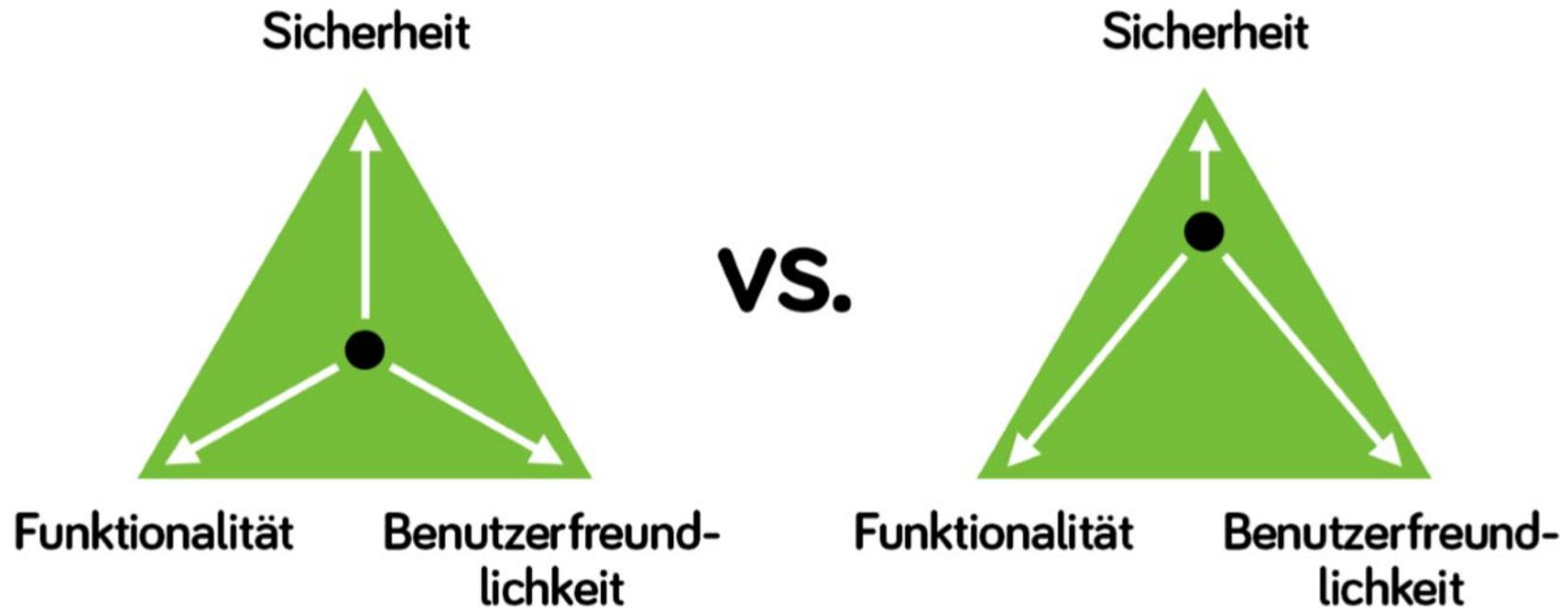


Ein Beispiel: Projektwettbewerb III

Ihr Verlust:

- Minus 2 Tage Zeit für den Wettbewerb
- 2 Tage Betriebsausfall
- Ihre Daten sind nicht mehr vertraulich, sondern öffentlich.
- Die Öffentlichkeit, auch Ihre Kunden, haben Kenntnis von Ihrem Datenverlust. Der Name des Unternehmens wird eine Zeitlang mit dem Datenverlust in Verbindung gebracht.

Ihr Risikomanagement



Quelle: Waite, A. InfoSec Triads: Security/Functionality/Ease-of-Use. June 12, 2010



Beispiel Home Office: Potenzielle Auswirkungen

Betrieb

- Gesunde Mitarbeitende
- Flexibilität
- Attraktiver Arbeitgeber
- Haftung (?)

Sicherheit

- Ungeschützte Zugänge
- Vermischung geschäftlicher und privater Geräte
- Ungeschützter Datentransfer
- Ungenügend sensibilisierte Mitarbeitende



Cybersicherheit ist Chefsache

- Ganzheitliche und immer wiederkehrende Auseinandersetzung mit dem Thema; Steuerung des strategischen Unternehmensrisikos.
- Umsetzung grundlegender Massnahmen: Patchen von Systemen, um Schwachstellen zu beheben, sowie regelmässige Backups.
- Wie reagieren wir im Notfall? Sind wir vorbereitet? Haben wir einen Notfallplan, ein Krisenkommunikationskonzept, eine Krisenorganisation und einen Notfallkontakt?
- Umsichtiges Verhalten aller Mitarbeitenden zum Schutz vor Cyberrisiken. Aufmerksamkeit für mögliche Risiken erhöhen. Hilfe zur Selbsthilfe, eigenverantwortliches Handeln.
- Integration der Sicherheit in Betrieb und Unternehmenskultur.



Besten Dank für Ihre Aufmerksamkeit