Startklar für Bedrohungen: Basissicherheit für Ihr KMU

7. Dezember 2023

CySeReS KMU Webinar

Dr. Thomas Stubbings, MBA

Teil 1: Wozu Cybersicherheit?

Cybersecurity im Kontext globaler Risiken

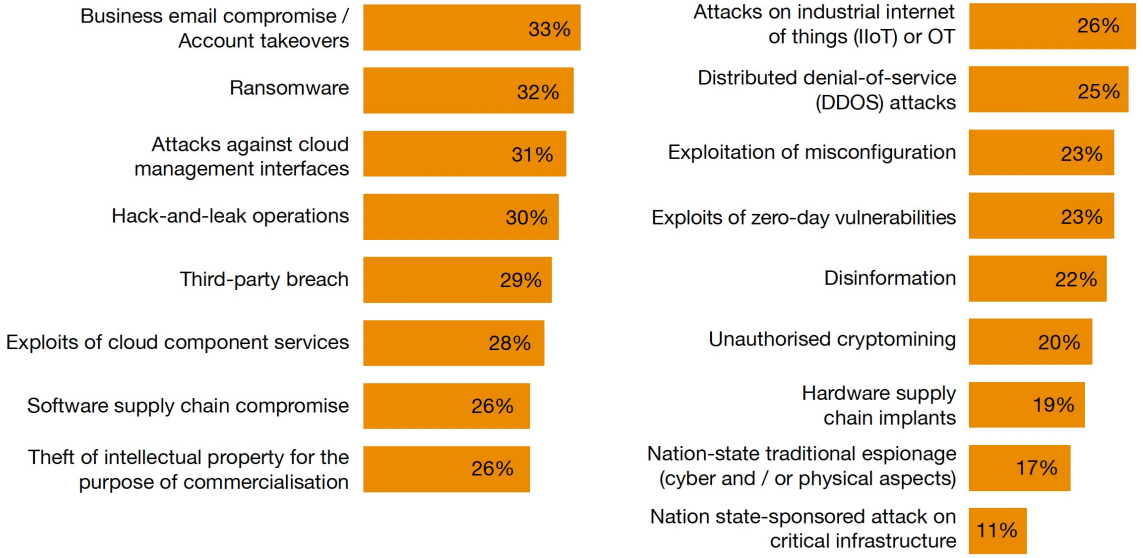
Quelle: World Economic Forum, Global Risk Report 2022

Was sind die Hauptbedrohungen?

ENISA Threat Landscape 2022 - Hauptbedrohungen

Quelle: ENISA, Threat Landscape 2022

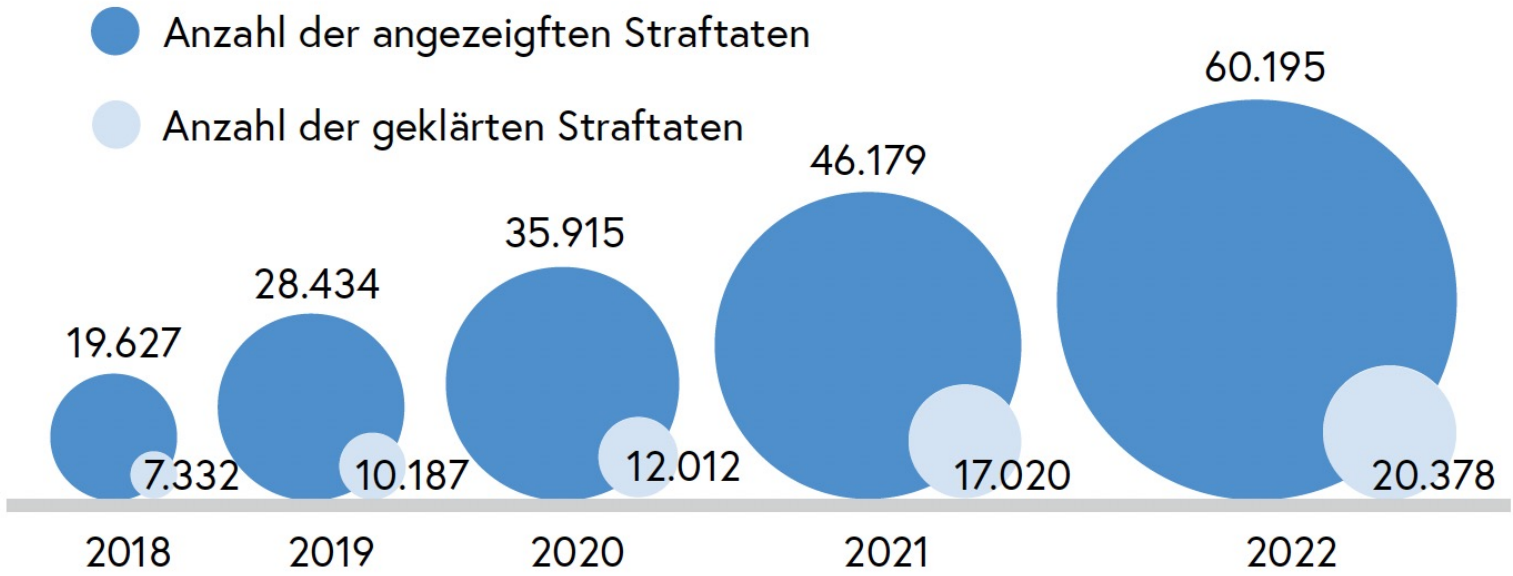
Hauptbedrohungen aus Sicht der Unternehmen



Quelle: PwC 2023 Global Digital Trust Report

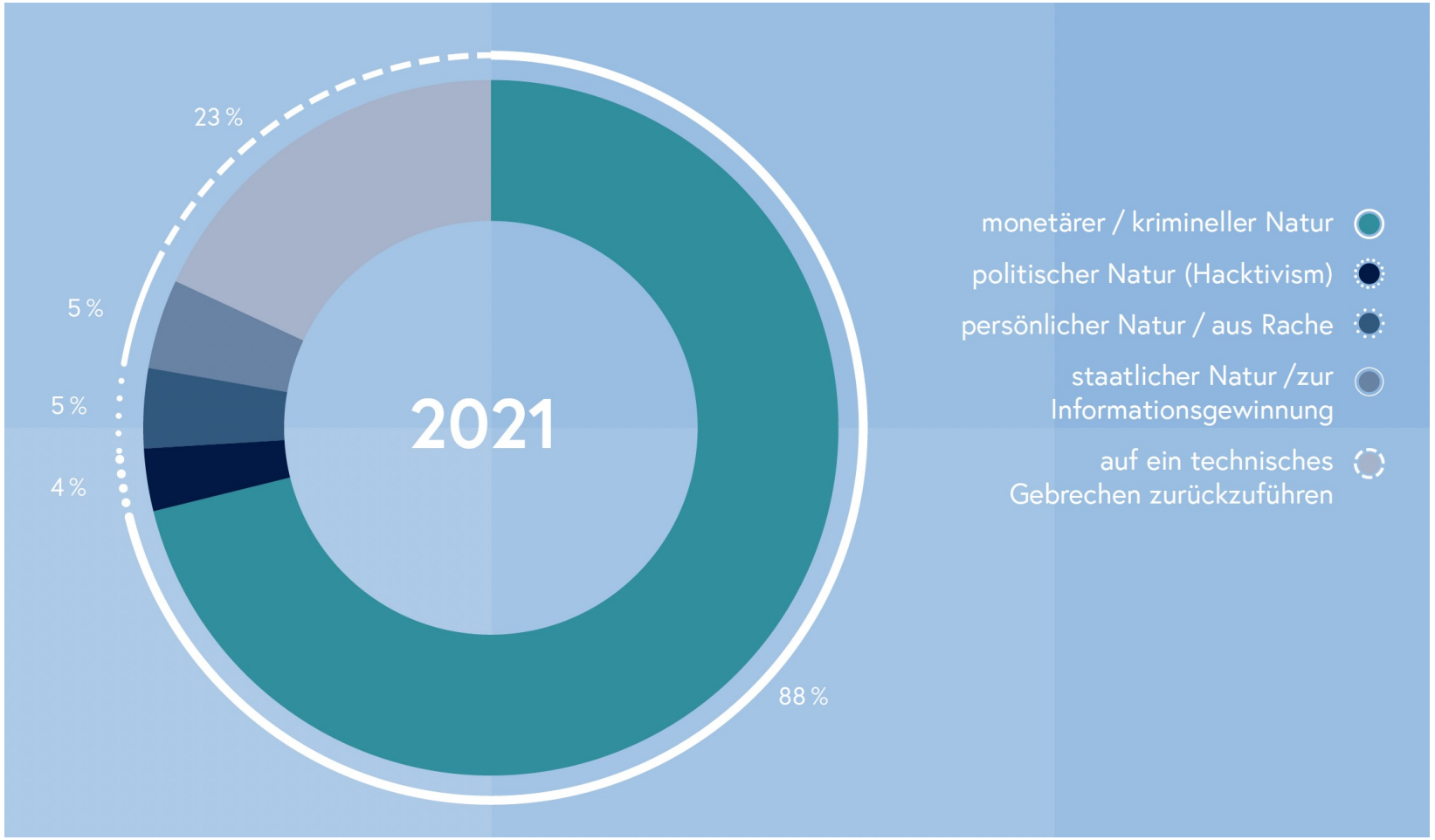
Cybercrime Entwicklung in Österreich

Entwicklung der angezeigten und geklärten Cybercrime-Fälle von 2018 bis 2022 in Österreich



Quelle: Bundeskriminalamt, Cybercrime Report 2022

Ursachen für Sicherheitsvorfälle



Quelle: Bundeskanzleramt, Cybersicherheitsbericht 2021

Auswirkungen & Schäden

1. Cyberangriffe sind mittlerweile zur Routine für österreichische Unternehmen geworden: In den letzten zwölf Monaten war jedes der von uns befragten Unternehmen zumindest ein Mal Ziel von einem Cyberangriff.

2. Nach wie vor herrscht große Verschlossenheit bei Unternehmen über Cyberattacken und Lösegeldzahlungen.

3. Betriebsausfälle und -unterbrechungen nach einem Cyberangriff haben mitunter eine Dauer von über vier Wochen. Damit stellen sie eine klare Existenzbedrohung für viele Unternehmen dar und sind mit enormen Schäden verbunden.

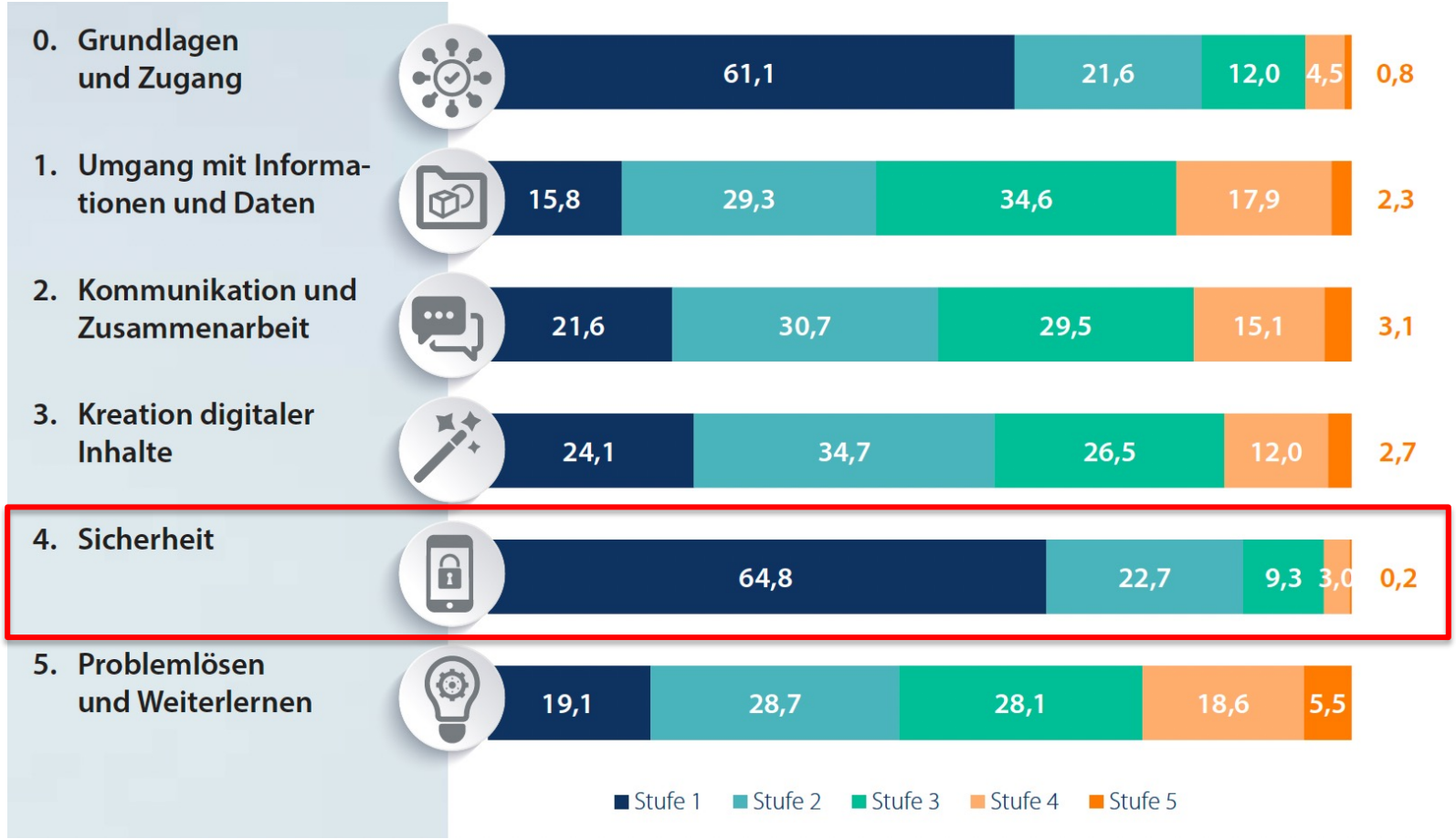
1. Der finanzielle Schaden durch Cyberangriffe beläuft sich bei rund 12 Prozent der Unternehmen auf über EUR 1 Mio.

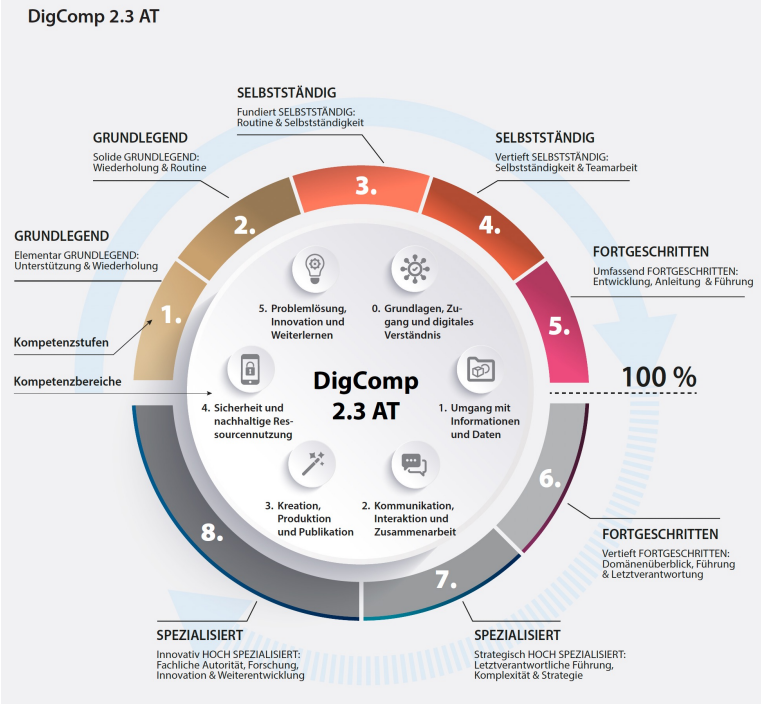
2. Bei drei Viertel der Unternehmen ist das Budget für Cybersecurity in den letzten zwölf Monaten gestiegen. Oftmals waren Cyberangriffe ein Mitauslöser dafür.

3. Ein Großteil der Unternehmen hat die interne Krisenplanung für Cyberangriffe erst nach einem Sicherheitsvorfall verbessert. Unternehmen muss die Wichtigkeit einer internen Krisenplanung bewusst werden, um Schäden durch Angriffe möglichst gering zu halten.

Quelle: KPMG Cybersecurity Studie AT, 2023

Kompetenzen - unterentwickelt





Quelle: Fit4Internet Jahresbericht, BMF (2023)

Immer professionelleres Office-365-Phishing

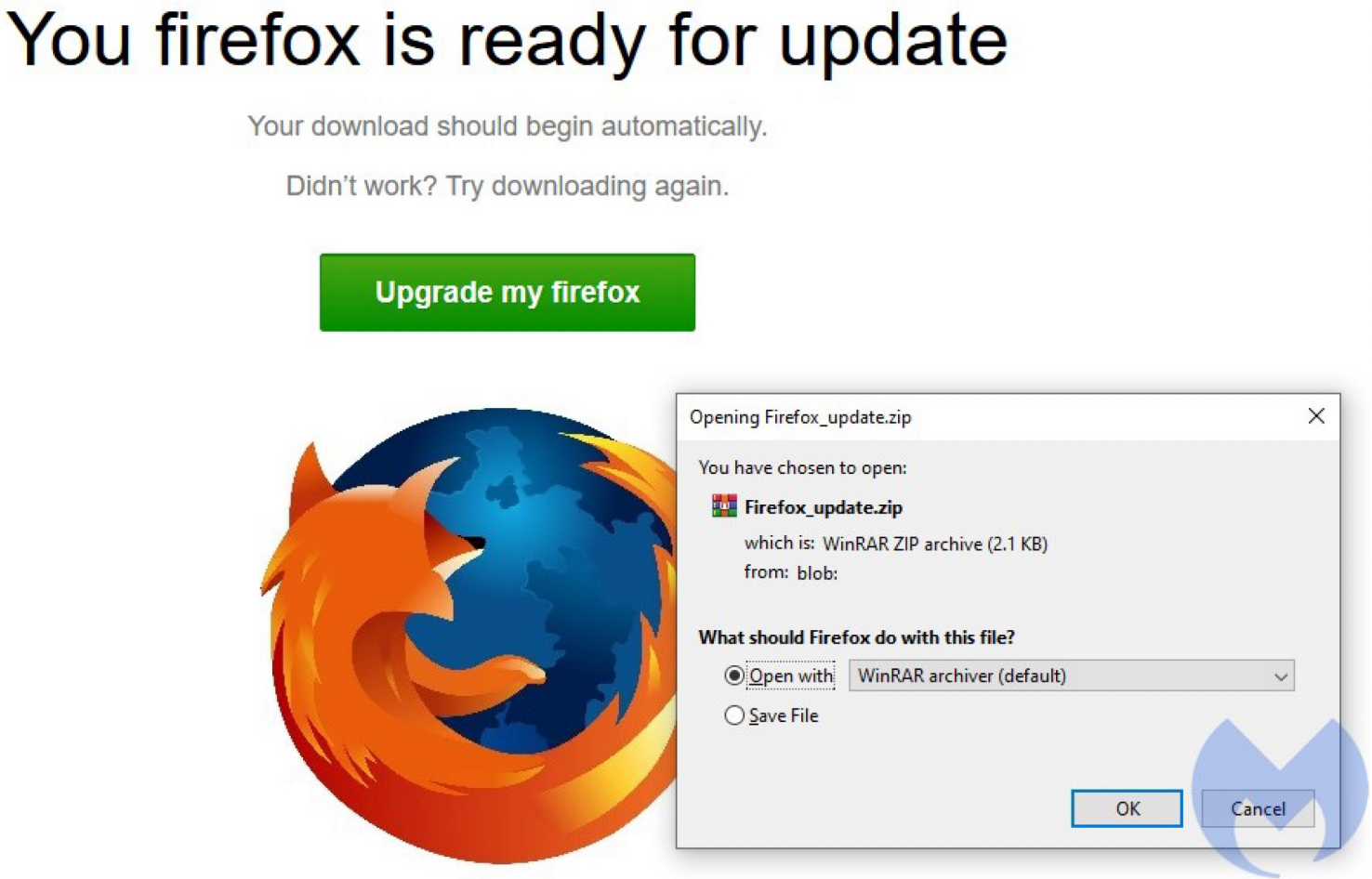
Angeblicher Projektvorschlag, der von einem Server heruntergeladen werden soll. Im Hintergrund wird ein Dokument verschwommen angezeigt. Um dieses zu öffnen, müsse allerdings zuerst das Office-365-Passwort eingegeben werden.

Die Unsicherheit der Passwörter

Top Ten der beliebtesten Passwörter

10. 123123
9. 111111
3. qwerty
2. 123456789
1. 123456

Schadsoftware via Fake Software / Fake Updates



Fake-Update (Quelle: Malwarebytes.com)

Hauptursache: Schwachstellen

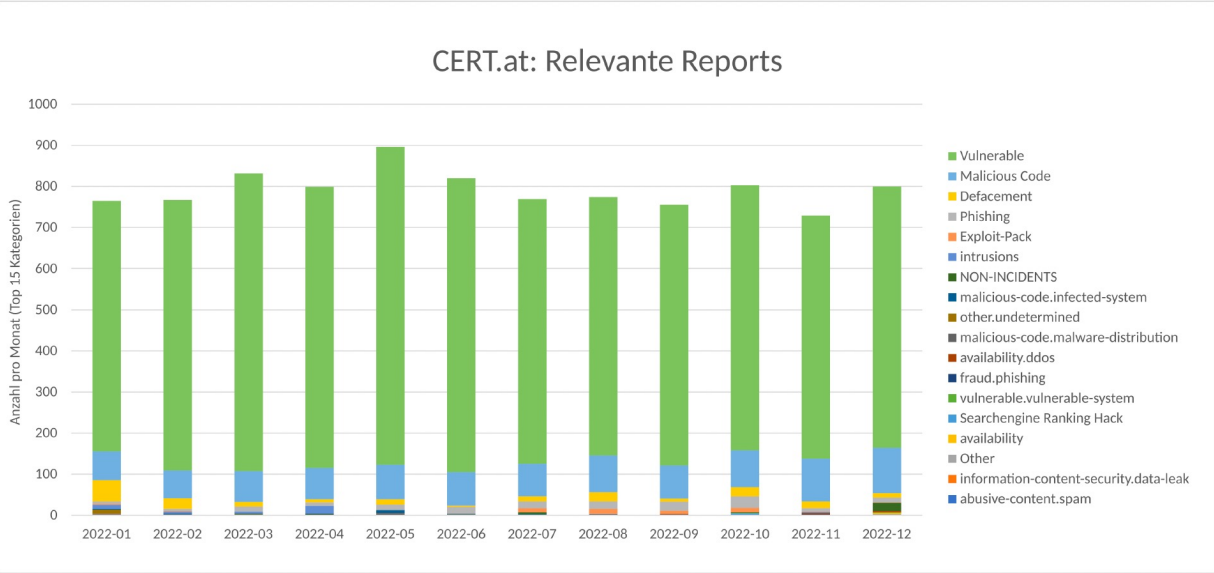


Abbildung 2.4: Incident Reports

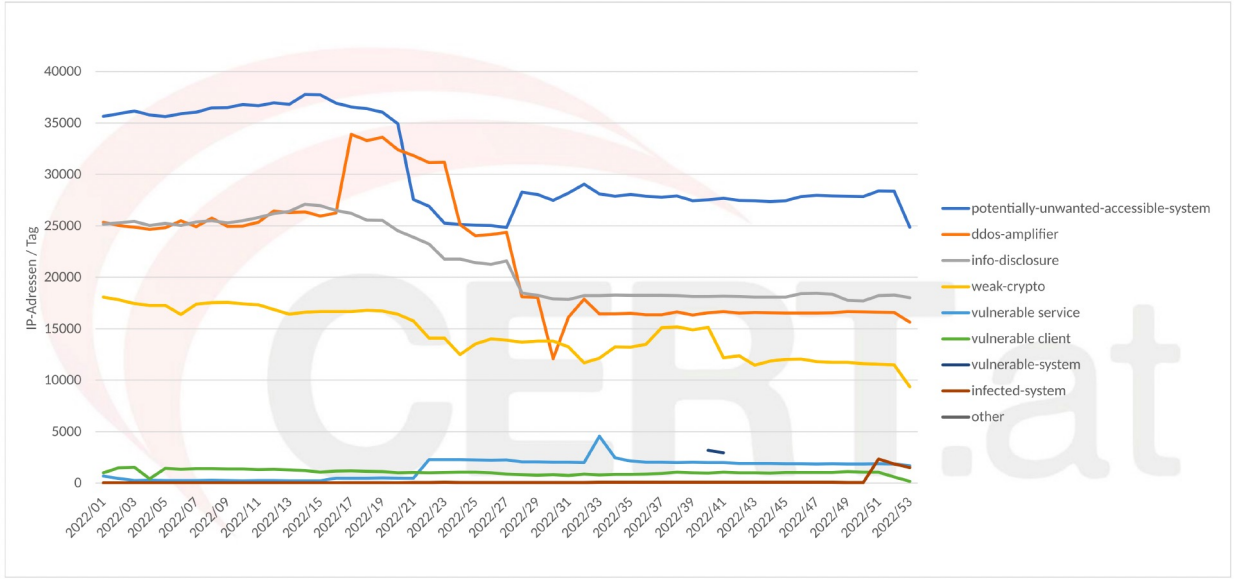
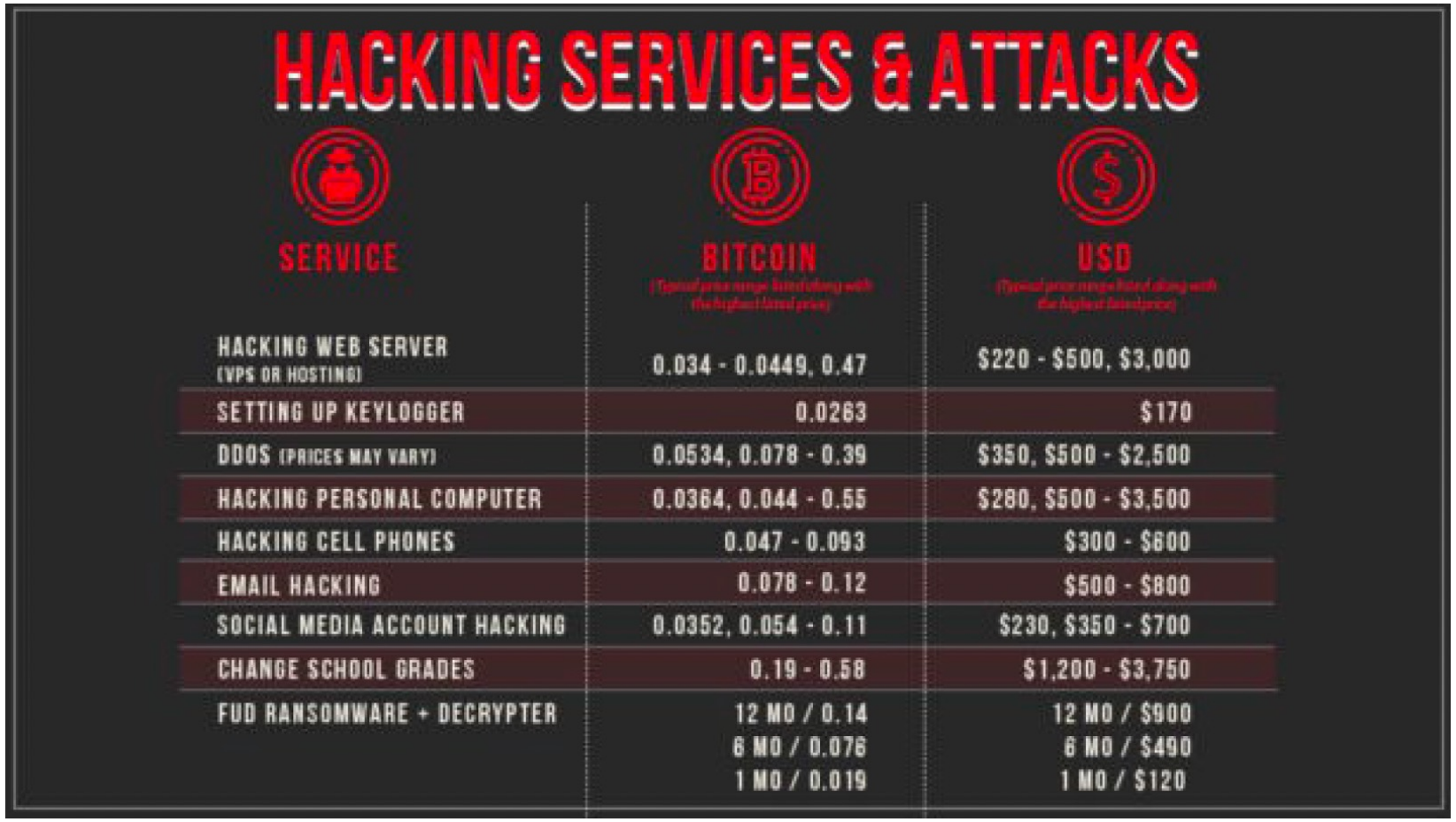


Abbildung 2.8: Alle Events der Taxonomie “vulnerable”

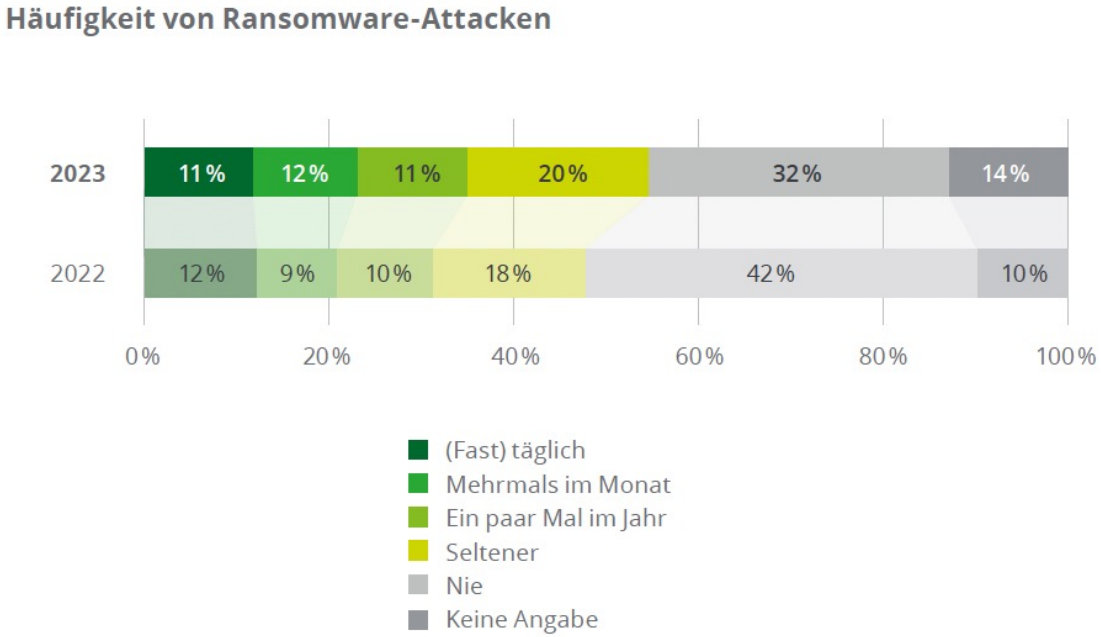
Quelle: CERT.AT, Jahresbericht 2022

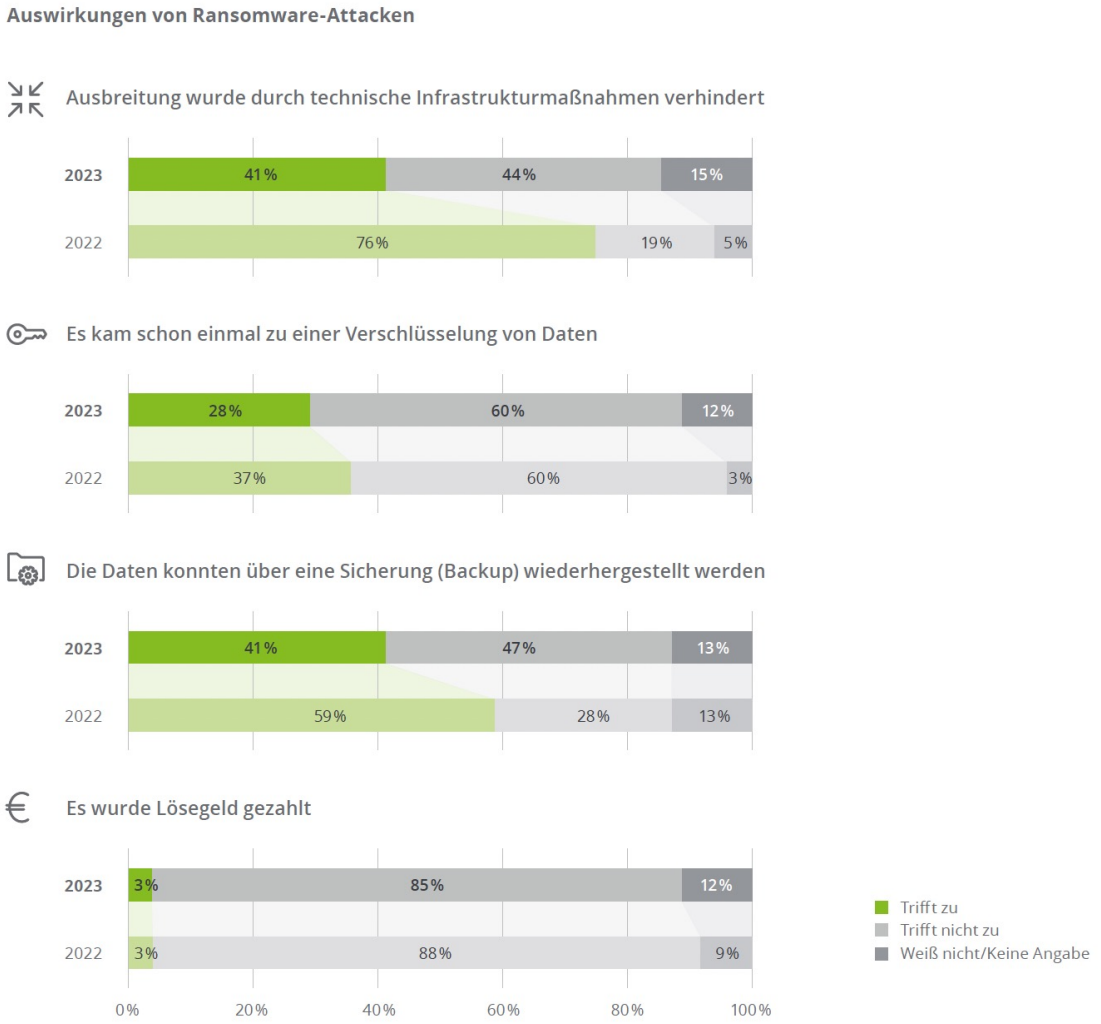
Das Dark Web – Crime as a Service



Source: Dark Web, SecPlicity: Security Simplified

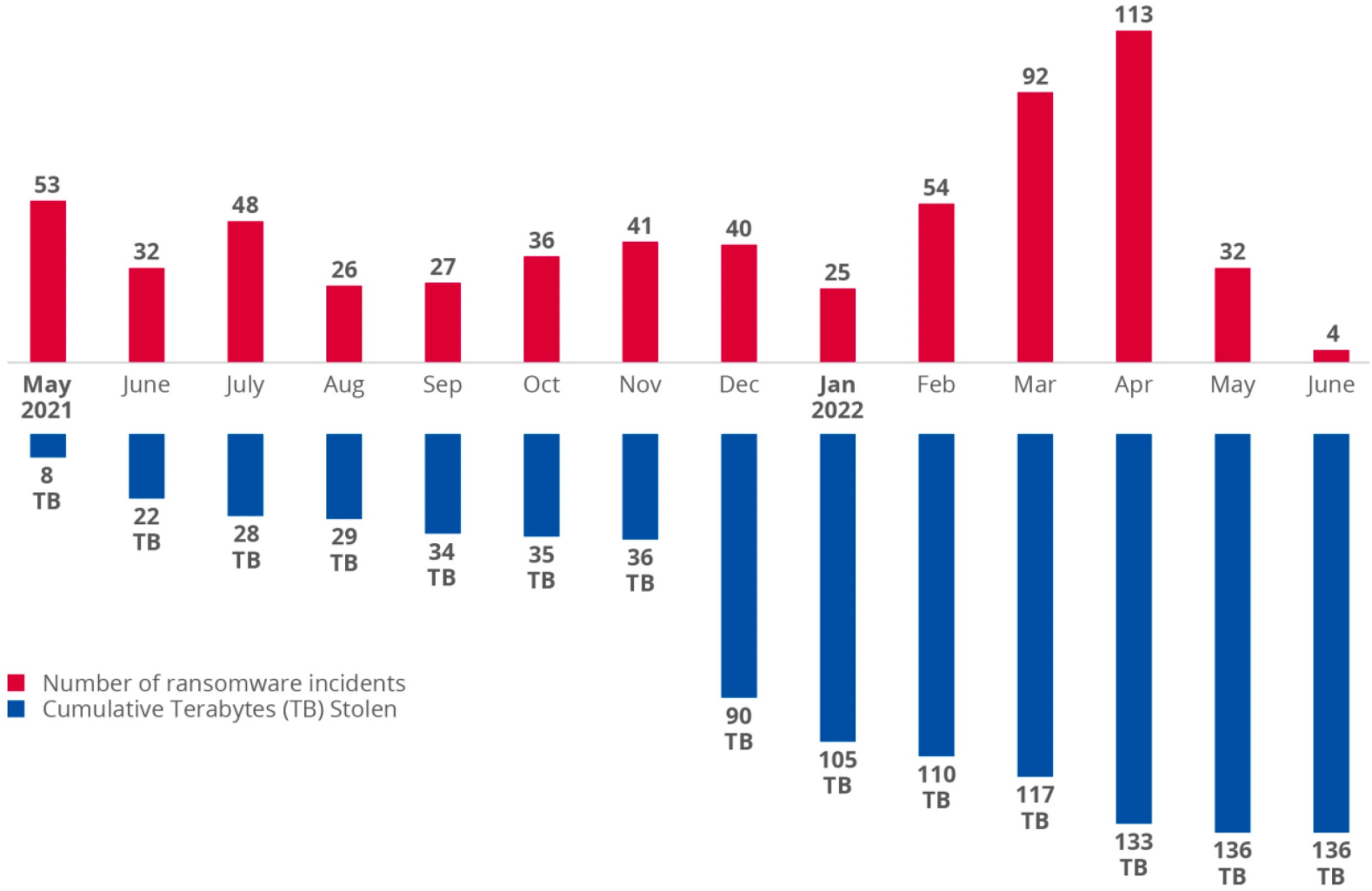
Ransomware – die alltägliche Bedrohung





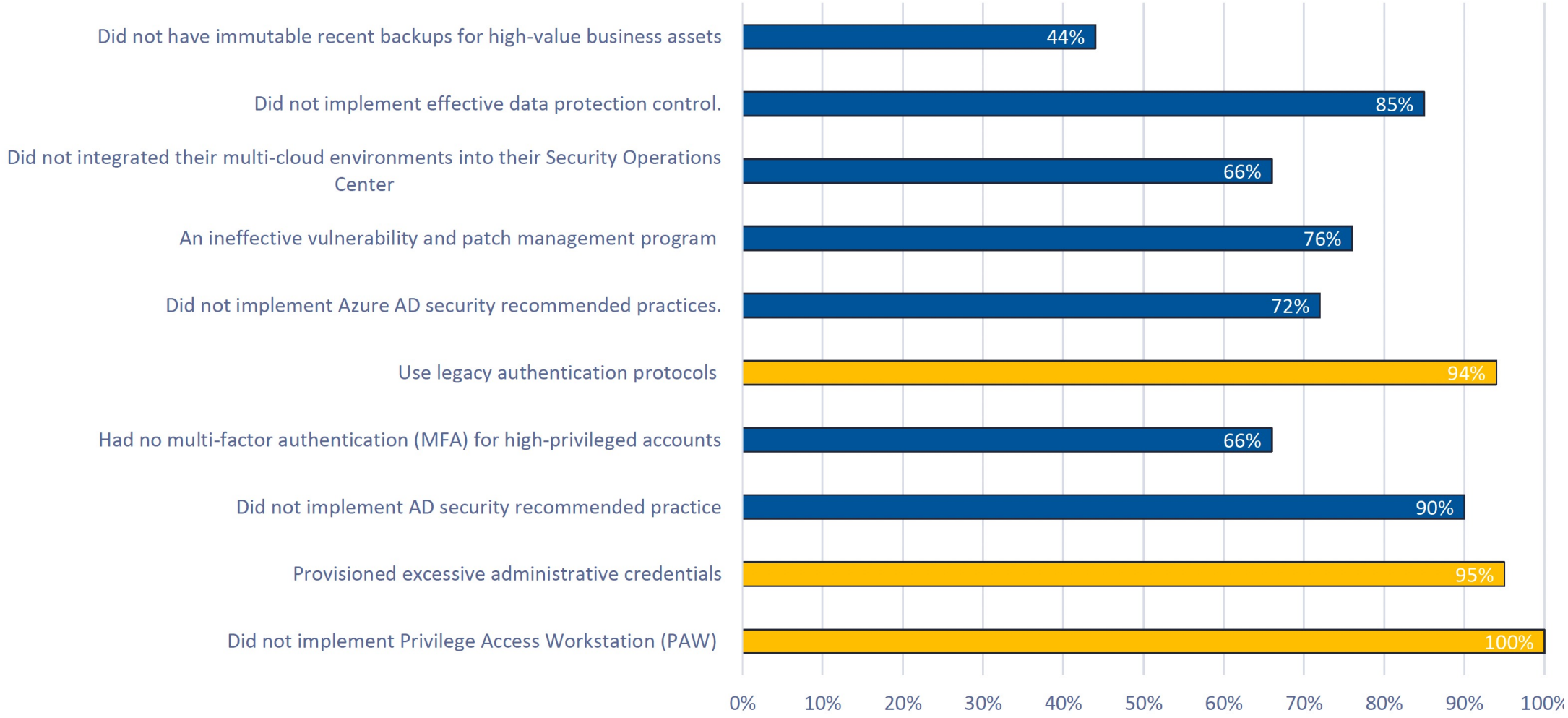
Quelle: Deloitte Cybersecurity Report AT 2023

Ransomware – Double Extortion



Quelle: ENISA, Threat Landscape 2022

Gründe für erfolgreiche Angriffe



Quelle: Microsoft, RSA Konferenz 2023

Teil 2: Was kann man tun um sich zu schützen

Basis-Sicherheitsanforderungen = Technisch / Organisatorische Maßnahmen

CYBER TRUST AUSTRIA

Vertraulichkeit

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Verschlüsselung

Integrität

- Dokumentation / Baseline
- Protokollierung
- Monitoring
- Forensik

Verfügbarkeit

- Resilienz-Strategie & Notfallpläne
- RTO / RPO für kritische Anwendungen
- Backup/Recovery-Tests
- Technische Schutzmaßnahmen
- Vulnerability & Patch-Management
- Security Checks & Tests

Allgemeines

- Policies
- Mitarbeiter-Schulung
- Verantwortlichkeiten

Informationssicherheits-Politik

Ziel

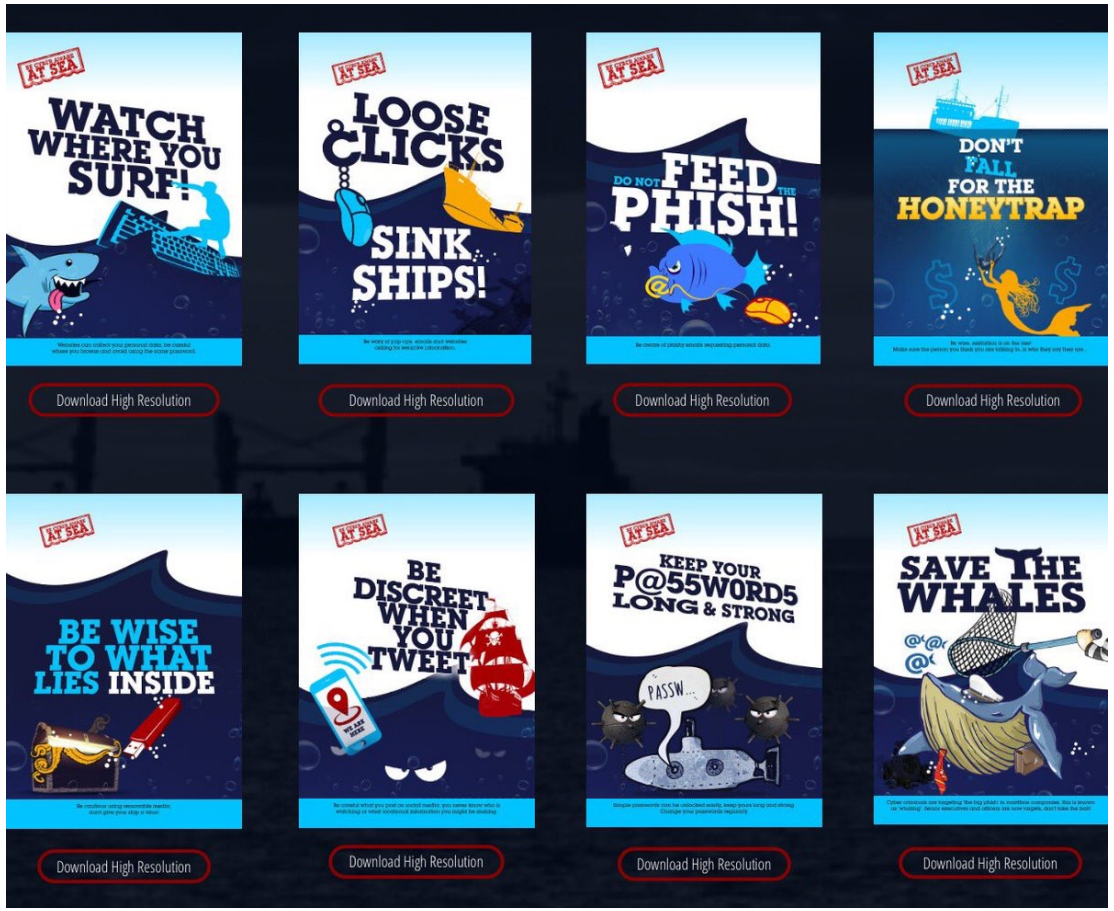
Die Geschäftsleitung bietet Anleitung und Unterstützung zur Informationssicherheit in Übereinstimmung mit den geschäftlichen Anforderungen und den einschlägigen Gesetzen und Vorschriften.

Maßnahmen

- Es sollte eine Informationssicherheitsrichtlinie erstellt, von der Geschäftsleitung genehmigt, herausgegeben und den Mitarbeitern und relevanten externen Parteien bekannt gemacht werden.
- Die Richtlinien sollten auf einem bestehenden Standard beruhen (z.B. ISO 27002, NIST 800, BSI IT-Grundschutz, IT-Sicherheitshandbuch der WKO, usw.)
- Die Themen sollten mindestens die folgenden Bereiche abdecken:
  - Sicherer Umgang mit IT-Infrastruktur und Informationen (einschließlich Datenschutz)
  - Richtige Auswahl und Verwaltung von Passwörtern
  - Internet-Sicherheit
  - E-Mails, Spam und Phishing
  - Gefährliche Malware
  - Reaktion auf vermutete IT-Sicherheitsvorfälle
- Die Richtlinien zur Informationssicherheit sollten in regelmäßigen Abständen oder bei wesentlichen Änderungen überprüft werden, um sicherzustellen, dass sie noch aktuell, angemessen und wirksam sind.

Schulungen zum Sicherheitsbewusstsein

- Das Hauptziel der Sensibilisierungskampagne ist die Bereitstellung positiver Informationen und Anleitungen zum Thema Informationssicherheit
- Die Kampagne sollte möglichst alle Mitarbeiter ansprechen und positiv wahrgenommen werden
- Sie soll das Interesse an dem Thema wecken
  - Von den Betroffenen zu den Beteiligten!
- Um eine Verbindung zwischen dem Thema Sicherheit und den für die Menschen wichtigen Gefühlen (intrinsische Motivation) herzustellen, ist es notwendig, gezielt auf die Motivatoren der Menschen einzugehen. Dazu gehören:
  - Einfühlungsvermögen/Gefühle (Zugehörigkeit)
  - Freude / Spaß (Humor)
  - Neugierde (Interesse an dem Thema)
  - Ehrgeiz (Beitrag zum Ganzen)
- Um dies erreichen zu können, bedarf es einer gut vorbereiteten, ansprechenden Marketingkampagne mit geeigneten Themen, die
  - sich in den Kontext des Unternehmens einfügt und dessen Kultur berücksichtigt
  - spricht die Mitarbeiter an und "bewegt" sie positiv
  - das Thema Sicherheit angemessen vermittelt hat



→ **Bewusstseinsbildung muss bereits bei Arbeitsbeginn erfolgen und in regelmäßigen Abständen erneuert werden.**

Verantwortlichkeiten

Ziel
Es gibt einen definierten Verantwortlichen für das Thema Informationssicherheit.

Maßnahmen
- Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben.
- Diese Tätigkeit kann speziell in kleineren Unternehmen auch neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.

Asset Verwaltung

Ziel
Die Werte der Organisation werden ermittelt und es werden angemessene Verantwortlichkeiten für ihren Schutz festgelegt.

Maßnahmen
- Informationen und andere Assets im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen sollten aufgezeichnet werden, und es sollte ein Inventar dieser Werte erstellt und gepflegt werden.
- Es sollte für alle Werte, die im Inventar geführt werden, eine Person geben, die dafür verantwortlich ist.
- Es sollten Regeln für die zulässige Nutzung von Informationen und Werten im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen aufgestellt, dokumentiert und angewendet werden.

Identitäts- und Zugangsmanagement

Ziel

Es wird sichergestellt, dass nur befugte Benutzer Zugang zu den Systemen und Diensten haben und dass ein unbefugter Zugriff verhindert wird.

Maßnahmen

- Es sollte ein formales Verfahren für die Registrierung und Deregistrierung von Benutzern eingeführt werden, um die Zuweisung von Zugriffsrechten zu ermöglichen.
- Verwendung eindeutiger Benutzerkennungen, damit die Benutzer mit ihren Handlungen in Verbindung gebracht und zur Verantwortung gezogen werden können.
- **Need-to-know /** Need-to-do-Prinzip:
  - Sie erhalten nur Zugang zu den Informationen, die Sie zur Erfüllung Ihrer eigenen Aufgaben benötigen (unterschiedliche Aufgaben / Funktionen bedeuten unterschiedliche Berechtigungen und damit ein anderes Zugangsprofil)
- Standardmäßig KEIN Zugriff (**Prinzip der Verweigerung**):
  - **Wenn** einem Subjekt **nicht ausdrücklich** Zugang zu einem Objekt gewährt wird, wird ihm der Zugang **per default** verweigert.
- Sofortige Deaktivierung oder Löschung der Kennungen von Benutzern, die die Organisation verlassen haben
- Privilegierte Zugriffsrechte sollten Benutzern nur bei Bedarf gewährt werden
  - Es sollte ein Genehmigungsverfahren und eine aktuelle Liste aller privilegierten Zugangsrechte geben.

Sichere Authentifizierung

Ziel

Der Zugang zu Informationen und Informationsverarbeitungssystemen wird durch ein sicheres Anmeldeverfahren kontrolliert.

Maßnahmen

Es sollte eine geeignete Authentifizierungsmethode gewählt werden, um die Identität des Benutzers zu bestätigen.

Beweisen, wer man zu sein behauptet, kann man in der Regel mit einer der folgenden 3 Eigenschaften:

- Etwas, das Sie kennen
- Etwas, das Sie haben
- Etwas, das Sie sind

Was spricht dagegen, nur eine dieser Methoden anzuwenden?

➔ Jede einzelne Methode ist für sich genommen schwach.

Starke Authentifizierung ist die Kombination von zwei oder mehr dieser Merkmale und wird **sehr empfohlen**!

Starke Authentifizierung bietet ein **deutlich** höheres Maß an Sicherheit.

Starke Authentifizierung wird auch als **Multi-Faktor-Authentifizierung (MFA)** bezeichnet.

- Passwörter
  - Einfache Passwörter
  - Einmalige Passwörter
- Biometrische Daten
  - Fingerabdruck
  - Iris-Scan
  - Spracherkennung
  - Tastatur-Dynamik
  - ...
- Wertmarken
- Chipkarten
- Digitale Signaturen

E-Mail-Sicherheit

- E-Mail gibt es schon seit langem, und das SMTP-Protokoll bietet KEINE Sicherheit. Es wurde davon ausgegangen, dass alle, die E-Mail verwenden, einfach ehrlich sein würden. Als solches bietet SMTP:
  - Keine Authentifizierung
  - Keine Verschlüsselung
- Die E-Mail war nicht einmal dazu gedacht, etwas Fortschrittliches (wie Bilder, Töne, Word-Dokumente) zu versenden. Sie war nur dazu gedacht, Text zu versenden.
- E-Mail ist aber heute für Unternehmen ein wichtiges, geschäftskritisches Kommunikationsmittel. Das führt zu folgenden Problemen:
  - Gefälschte E-Mail
  - Manipulierte E-Mail
  - Kompromittierung vertraulicher Informationen, die per E-Mail verschickt werden
  - Per E-Mail verbreitete Malware
  - SPAM

- Die Lösung - Verschlüsselung:
  - Zertifikatsbasierend (S/MIME, PGP)
  - Sichere Austauschplattformen (OneDrive)
  - „symmetrische Verschlüsselung“ (zB. verschlüsseltes ZIP-File)

Schutz vor Malware

Ziel
Informationen und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.

Maßnahmen

a) Es sollten Erkennungs-, Präventions- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Nutzer durchgeführt werden.
b) Installation und regelmäßige Aktualisierung von Software zur Erkennung und Entfernung von Malware für die routinemäßige Überprüfung von Computern und Medien
c) Erstellung geeigneter Notfallmanagement- und Geschäftskontinuitätspläne für die Wiederherstellung nach Malware-Angriffen, einschließlich aller erforderlichen Daten, einer Software-Sicherung und Vorkehrungen für die Wiederherstellung

- Viren
- Trojaner
- Würmer
- SPAM
- Spyware
- Rootkit
  - Sitzt unterhalb des Betriebssystems - schwer zu erkennen!
- Kryptolockers
  - Sehr störend
- Mobile Malware
  - Hybride Infektionen
- Driveby-Malware
  - Keine Benutzerinteraktion erforderlich
  - "Wasserlochangriffe"
  - "Mouseover-Angriff"

Härtung des Systems

- Ändern Sie Standardkennwörter!
- Unnötige Konten entfernen oder deaktivieren
- Deaktivierte Dienste/Software entfernen
- Compiler entfernen
- Dienste als eingeschränkte Konten führen
- Konfigurieren Sie Dienste für maximale Sicherheit
- Konfigurieren Sie die Betriebssystemeinstellungen für maximale Sicherheit
- Installieren Sie eine hostbasierte Firewall und pflegen sie die Regeln
- Beschränkung des physischen Zugangs
- Sperren von Netzwerkausrüstung und Zugang
- Sicherer Zugriff auf Wechselmedien

- Bzw. fordern sie dies von ihrem IT-Betreuer ein!

Schwachstellen- und Patch-Management

Ziel

Das Ausnutzen von technischen Schwachstellen wird verhindert.

Maßnahmen

- Es sollten rechtzeitig Informationen über technische Schwachstellen der eingesetzten Informationssysteme eingeholt, die Gefährdung der Organisation durch solche Schwachstellen bewertet und geeignete Maßnahmen zur Bewältigung des damit verbundenen Risikos getroffen werden.
- Wenn ein Patch aus einer vertrauenswürdigen Quelle verfügbar ist, sollten die mit der Installation des Patches verbundenen Risiken bewertet werden (die Risiken der Schwachstelle sollten gegen die Risiken der Installation des Patches abgewogen werden);
- Grundsätzlich sollten **Sicherheits-Patches so rasch wie möglich eingesetzt** werden
- Die Patches sollten vor der Installation getestet und bewertet werden, um sicherzustellen, dass sie die gewünschte Wirkung haben und keine unerwünschten Nebenwirkungen auftreten.
- Ist ein Patch nicht verfügbar, sollten andere Maßnahmen in Betracht gezogen werden, z. B.: Abschaltung der von der Schwachstelle betroffenen Dienste oder Funktionen; Anpassung oder Ergänzung der Zugangskontrolle, zB. Firewalls, an den Netzgrenzen; verstärkte Überwachung zur Aufdeckung von Angriffen; Sensibilisierung der Mitarbeiter für die Schwachstelle.
- Es sollte ein Verfahren für Situationen festgelegt werden, in denen eine Schwachstelle festgestellt wurde, aber keine geeignete Gegenmaßnahme existiert.

Protokollierung und Überwachung

Ziel
Die System-Ereignisse werden aufgezeichnet und Vorgänge werden nachvollziehbar.

Maßnahmen
- Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Vorfälle und Informationssicherheitsvorfälle aufzeichnen, sollten erstellt, aufbewahrt (und regelmäßig überprüft) werden.
- Logging-Einrichtungen und Log-Informationen sollten vor Manipulation und unberechtigtem Zugriff geschützt werden.
- Die Aktivitäten des Systemadministrators sollten aufgezeichnet werden, und die Protokolle sollten geschützt (und regelmäßig überprüft) werden.

Management von Zwischenfällen

Ziel

Ein kohärenter und wirksamer Ansatz für den Umgang mit Vorfällen im Bereich der Informationssicherheit, einschließlich der Meldung von Sicherheitsvorfällen und Schwachstellen, ist gewährleistet.

Maßnahmen

- Es sollten Zuständigkeiten und Verfahren für den Umgang mit Vorfällen im Bereich der Informationssicherheit festgelegt werden, um eine schnelle, wirksame und ordnungsgemäße Reaktion auf diese Vorfälle zu gewährleisten.
- Auf Vorfälle im Bereich der Informationssicherheit sollte **gemäß dokumentiertem Verfahren reagiert** werden.
- Die Verfahren sollten **getestet** werden
- Die Organisation sollte Verfahren zur Identifizierung, Erfassung, Aufzeichnung und Aufbewahrung von Informationen, die als Beweismittel verwendet werden können, einführen und anwenden.
- Die aus der Analyse und Behebung von Informationssicherheitsvorfällen gewonnenen Erkenntnisse sollten genutzt werden, um die Wahrscheinlichkeit des Auftretens oder die Auswirkungen künftiger Vorfälle zu verringern.

Management der Geschäftskontinuität

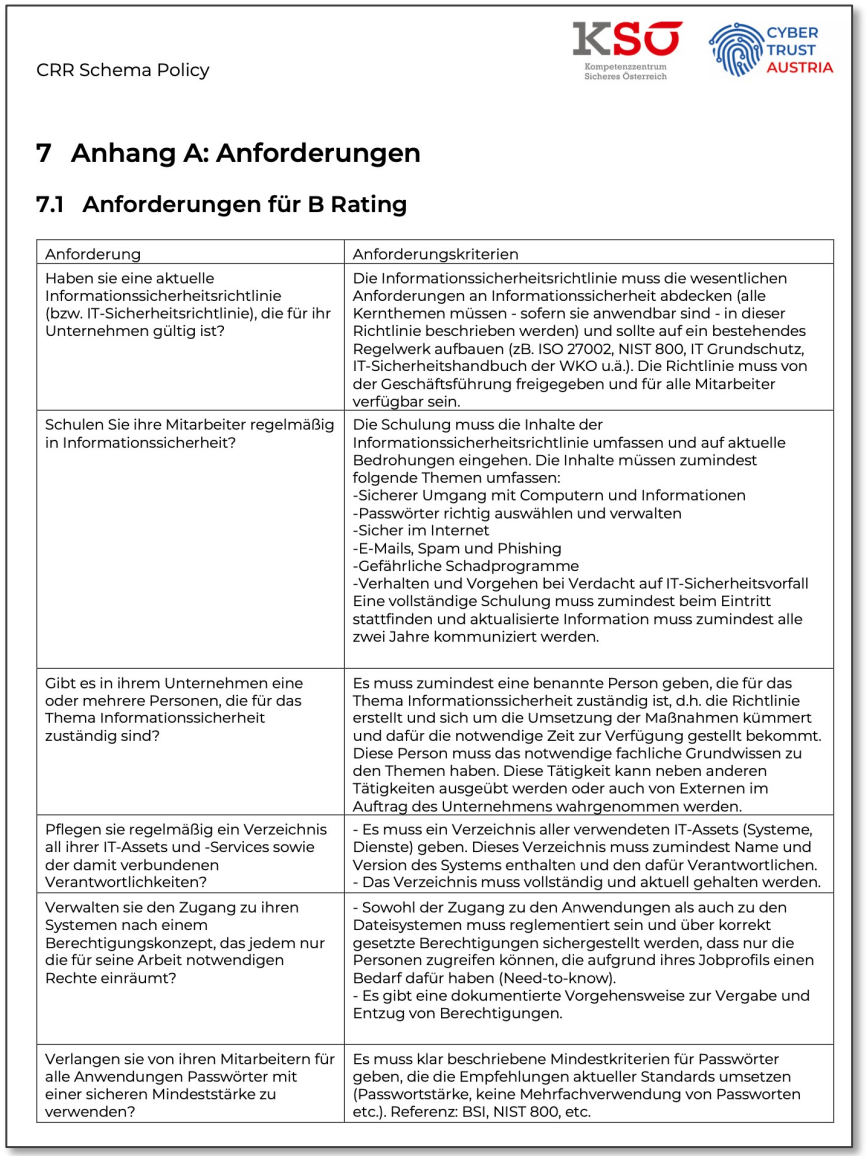
Ziel
Die Aufrechterhaltung der Informationssicherheit sollte in den Geschäftskontinuitätsplan (BCM) der Organisation eingebettet sein.

Maßnahmen
- Die Organisation sollte über BCM-Pläne für Katastrophen wie Systemausfälle, Malware-Infektionen (einschließlich Cryptolocker), Datenverluste usw. verfügen.
- **Sichern/Wiederherstellen**
  - Angemessene Sicherungseinrichtungen sollten vorhanden sein, um sicherzustellen, dass alle wichtigen Informationen und Softwareanwendungen nach einer Beschädigung oder einem Medienausfall wiederhergestellt werden können.
  - Backups sollten an einem Ort aufbewahrt werden, der weit genug entfernt ist, um den Hauptstandort vor Schäden zu schützen;
  - Die Datenschutzvorkehrungen für die einzelnen Systeme und Dienste sollten **regelmäßig überprüft und getestet** werden, um sicherzustellen, dass sie den Anforderungen der Geschäftskontinuitätspläne entsprechen.
- Die BCM-Maßnahmen und -Pläne sollten regelmäßig getestet werden.

Das Cyber Risk Rating Schema des KSÖ für Baseline Security

- **25 Anforderungen zur Bewertung von Cyber Risiken**
  - 14 Anforderungen für B-Rating (Base-Security)
  - 11 Anforderungen für A-Rating (Advanced-Security)

https://kompetenzzentrum-sicheres-oesterreich.at/wp-content/uploads/2022/09/CRR-Schema-Policy-2023-final.pdf



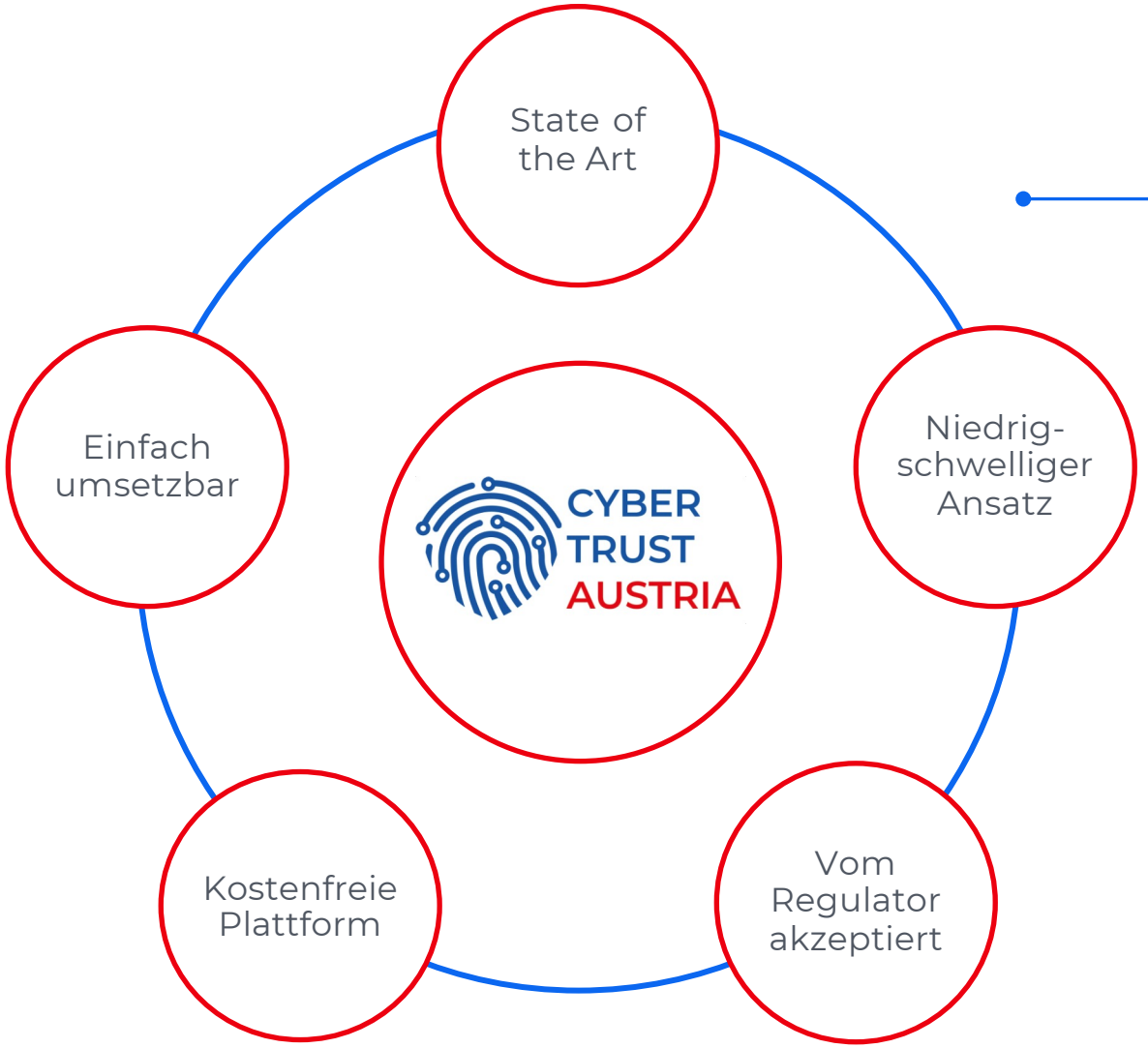
CRR Schema Policy

7 Anhang A: Anforderungen

7.1 Anforderungen für B Rating

Anforderung	Anforderungskriterien
Haben sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für ihr Unternehmen gültig ist?	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKO u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für alle Mitarbeiter verfügbar sein.
Schulen Sie ihre Mitarbeiter regelmäßig in Informationssicherheit?	Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen: -Sicherer Umgang mit Computern und Informationen -Passwörter richtig auswählen und verwalten -Sicher im Internet -E-Mails, Spam und Phishing -Gefährliche Schadprogramme -Verhalten und Vorgehen bei Verdacht auf IT-Sicherheitsvorfall Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.
Gibt es in ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit zuständig sind?	Es muss zumindest eine benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.
Pflegen sie regelmäßig ein Verzeichnis all ihrer IT-Assets und -Services sowie der damit verbundenen Verantwortlichkeiten?	- Es muss ein Verzeichnis aller verwendeten IT-Assets (Systeme, Dienste) geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen. - Das Verzeichnis muss vollständig und aktuell gehalten werden.
Verwalten sie den Zugang zu ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?	- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben (Need-to-know). - Es gibt eine dokumentierte Vorgehensweise zur Vergabe und Entzug von Berechtigungen.
Verlangen sie von ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?	Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, keine Mehrfachverwendung von Passworten etc.). Referenz: BSI, NIST 800, etc.

Das „Cyber Trust Austria“ Gütesiegel steht für Cybersicherheit in Unternehmen



Cyber Trust hilft Unternehmen durch einen - von der zuständigen Behörde akzeptierten – niedrigschwelligen, günstigen und dennoch aussagekräftigen Ansatz (das Cyber Trust Gütesiegel), einen gültigen Nachweis der Cybersicherheitsstandards zu erbringen und damit NIS 2 Unternehmen den gesetzeskonformen Nachweis ihres Lieferantenrisikomanagements.

Gütesiegel zum Nachweis der Cybersicherheit

	Label	Label Silber	Label Gold
Basis	KSV1870 Cyber Risk B Rating	KSV1870 Cyber Risk A Rating	KSV1870 Cyber Risk A+ Rating
Assurance Level	Validierte Selbstdeklaration	Validierte Selbstdeklaration	Validierte Selbstdeklaration plus externer Audit
	Beantwortung eines Fragebogens mit Validierung; Zustimmung zur möglichen Durchführung eines stich-probenartigen Überprüfungs-Audits, Durchführung eines automatisierten Web Risk Scoring.	Beantwortung eines Fragebogens mit Validierung; Zustimmung zur möglichen Durchführung eines stich-probenartigen Überprüfungs-Audits, Durchführung eines automatisierten Web Risk Scoring.	Durchführung eines Audits durch einen qualifizierten Prüfer (QuaSte-Akkreditierung) zur Prüfung der Evidenzen; Durchführung eines automatisierten Web Risk Scoring.
Security Claim	Baseline Security	Advanced Security	Advanced Security
Anzahl Kriterien	14	25	25
Gültigkeitsdauer	1 Jahr	1 Jahr	1 Jahr
Preis	890,-	1.290,-	1.390,-

Das Cyber Risk Schema wird von Experten gesteuert und von den Behörden akzeptiert

Am Cyber Risk Schema beteiligte Organisationen

KSÖ Kompetenzzentrum Sicheres Österreich
CYBER TRUST AUSTRIA
KSV1870

Unternehmen der kritischen Infrastruktur:

Banken
Gesundheit
Energie
Verkehr
Finanzmarktinfrastruktur
Digitale Infrastruktur
Trinkwasser
Öffentliche Verwaltung

Leitungsorgane der beteiligten Unternehmen und Vereine entsenden je einen Vertreter ↓ ↑ Bericht

Ein Vertreter für jeden Sektor ↓

Strategisch
(CRR-/Label-Schema)

Operativ
(CRR-/Label-Vergabe)

Cyber Risk Management Board

Erarbeitet Vorschläge für das CRR-Schema und das darauf basierende Cyber Trust Label

Eskalationsinstanz bei Unklarheiten bzgl. Rating und Qualifikation für Label

Prüfung nach Aussetzungen des Ratings / Labels

Schlägt vor →

← Beschließt

Jährlicher Bericht →

Cyber Risk Advisory Board

Definition Anforderungen

Beschluss des CRR-Schemas und des darauf basierenden Cyber Trust Labels

Kontrollinstanz

Im Bedarfsfall Korrekturen am Schema

KSÖ Kompetenzzentrum Sicheres Österreich

- Das Cyber Risk Advisory Board unter Führung des KSÖ verleiht dem Gütesiegel **Legitimität & Glaubwürdigkeit**
- Zusammensetzung aus **Vertretern der kritischen Sektoren** gemäß NIS-Gesetz:
  - Leitende Sicherheitsverantwortliche großer Unternehmen der kritischen NIS-Sektoren
- Weitere **Partner** aus unserem Cyber Ökosystem:
  - PwC
  - A1 Digital
  - K-Businesscom
  - SBA Research GmbH
  - CIS GmbH
  - Wiener Städtische Versicherung
  - u.a.m.

Wie kommt man zu einem Cyber Trust Label?

Online Beantragung

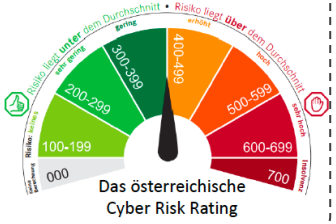
Beantwortung des Fragebogens

Automatisiertes Web Risk Scoring

Validierung der Antworten, Klärung von offenen Fragen

Risk Rating

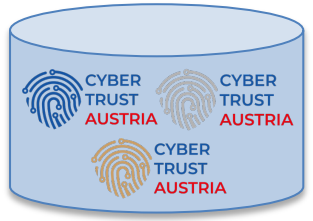
KSV1870
Risk Rating Engine



Auswahl des Audit Partners

Audit Partner überprüft das Rating mittels eines evidenzbasierten Audits

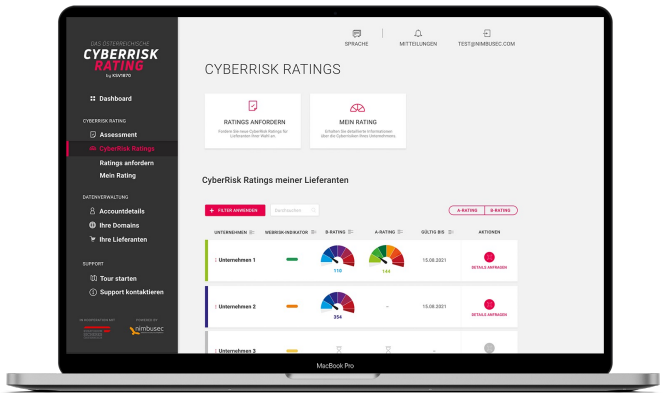
Vergabe des Labels* & Registrierung in der Cyber Trust Label Datenbank



* vorausgesetzt das Risk Rating ist <= 190

Das Cyber Trust Label ist Teil eines Security-Ökosystems

KSV1870 nimbusec website security & compliance



CyberRisk Rating

Tools

Services

CYBER RISK SCHEMA des KSÖ

Kompetenzzentrum Sicheres Österreich

Audits

Beratungsleistungen

Fortbildungen

Partner

CYBER TRUST AUSTRIA

CYBER TRUST AUSTRIA

CYBER TRUST AUSTRIA

Cyber Trust Label

CYBER TRUST EUROPE

Registered Union Trade Mark

Ihr Kontakt

CYBER TRUST AUSTRIA

Dr. Thomas Stubbings, MBA

Geschäftsführer

CTS Cyber Trust Services GmbH
Wienerbergstrasse 11 / 12A
A – 1100 Wien
+43 (1) 994 60 / 5454
+43 (664) 1036654
thomas.stubbings@cyber-trust.at
www.cyber-trust.at