WEIHRICH
INFORMATIK

CyberSecurity

pebeForum 2023

Überblick

- **Grundlagen** und Entstehung vom World Wide Web
- **Einführung** in Cyber Security
- **Entwicklung** von Cyber Security Vorfällen
- **Massnahmen**
- Abschluss und Empfehlung
- Fragen und Antworten

Ziel: Sensibilisierung zur Verbesserung Ihrer Sicherheit

Thomas Weihrich

- Lehre Maschinenmechanik an der MSW
- Studium der Informatik in Winterthur und Rapperswil
- Tätig in der Softwareentwicklung in den Bereichen Logistik und Echtzeit-Automation
- Gründung der Weihrich Informatik 2003 - Systemhaus
- Gesamtverantwortung für zahlreiche erfolgreiche IT-Projekte im In- und Ausland
- Hersteller Zertifizierungen und Unternehmenspreise für besondere Lösungen
- Microsoft Cloud Solution Provider Zertifizierungen
- ISO 9001 und ISO 27001:2022 zertifiziert

Grundlagen

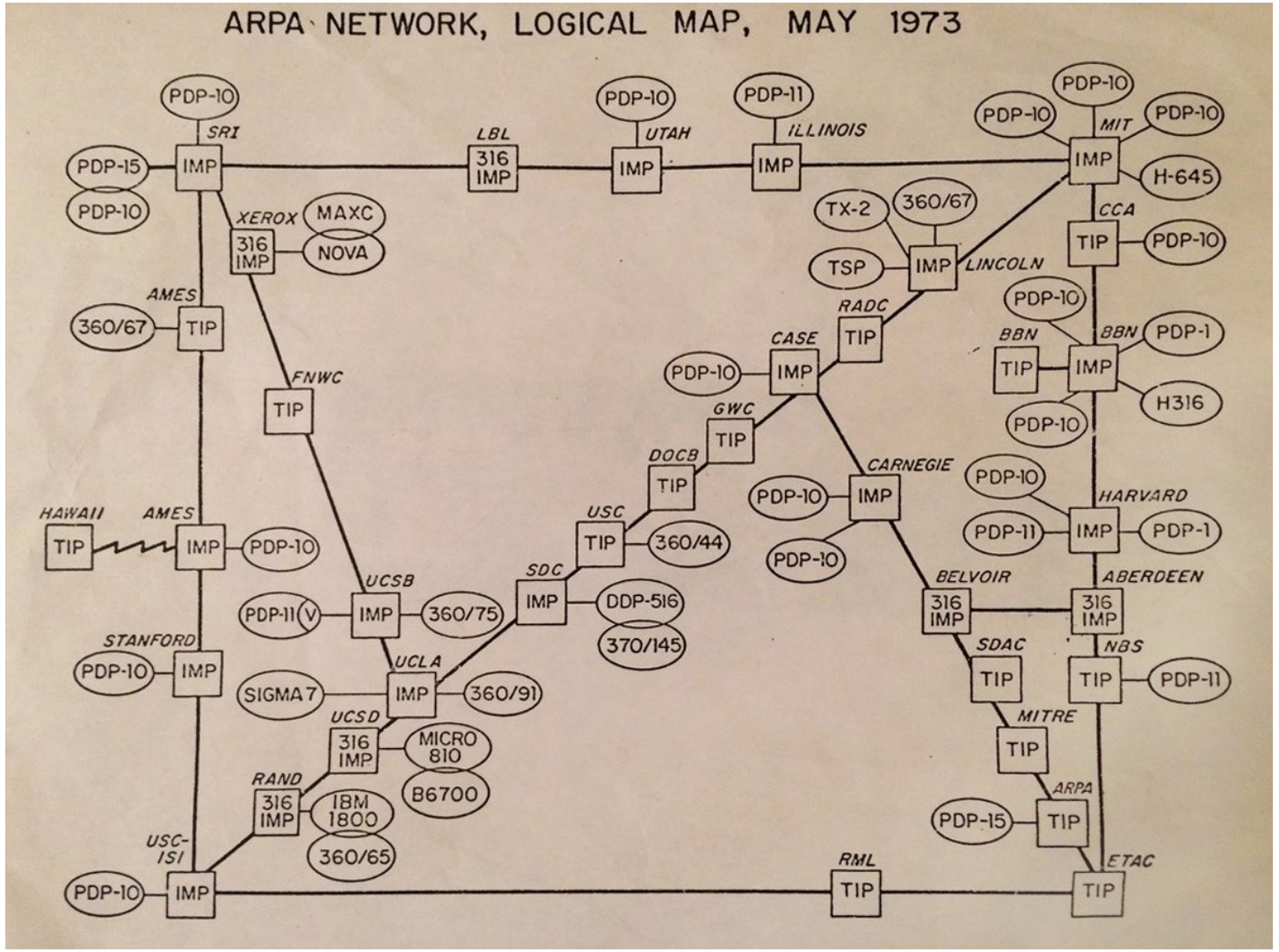
Entstehung vom Internet und World Wide Web

Erfindung des Internet


A WERNER HERZOG FILM
LO AND BEHOLD
REVERIES OF THE CONNECTED WORLD


INTERFACE
MESSAGE
PROCESSOR
Developed for
the Advanced Research Projects Agency
by Bolt Beranek and Newman Inc.
POWER
SENSE
REGISTER
MASTER
CLEAR
STORE
FETCH

ARPANET – Der Ursprung vom Internet

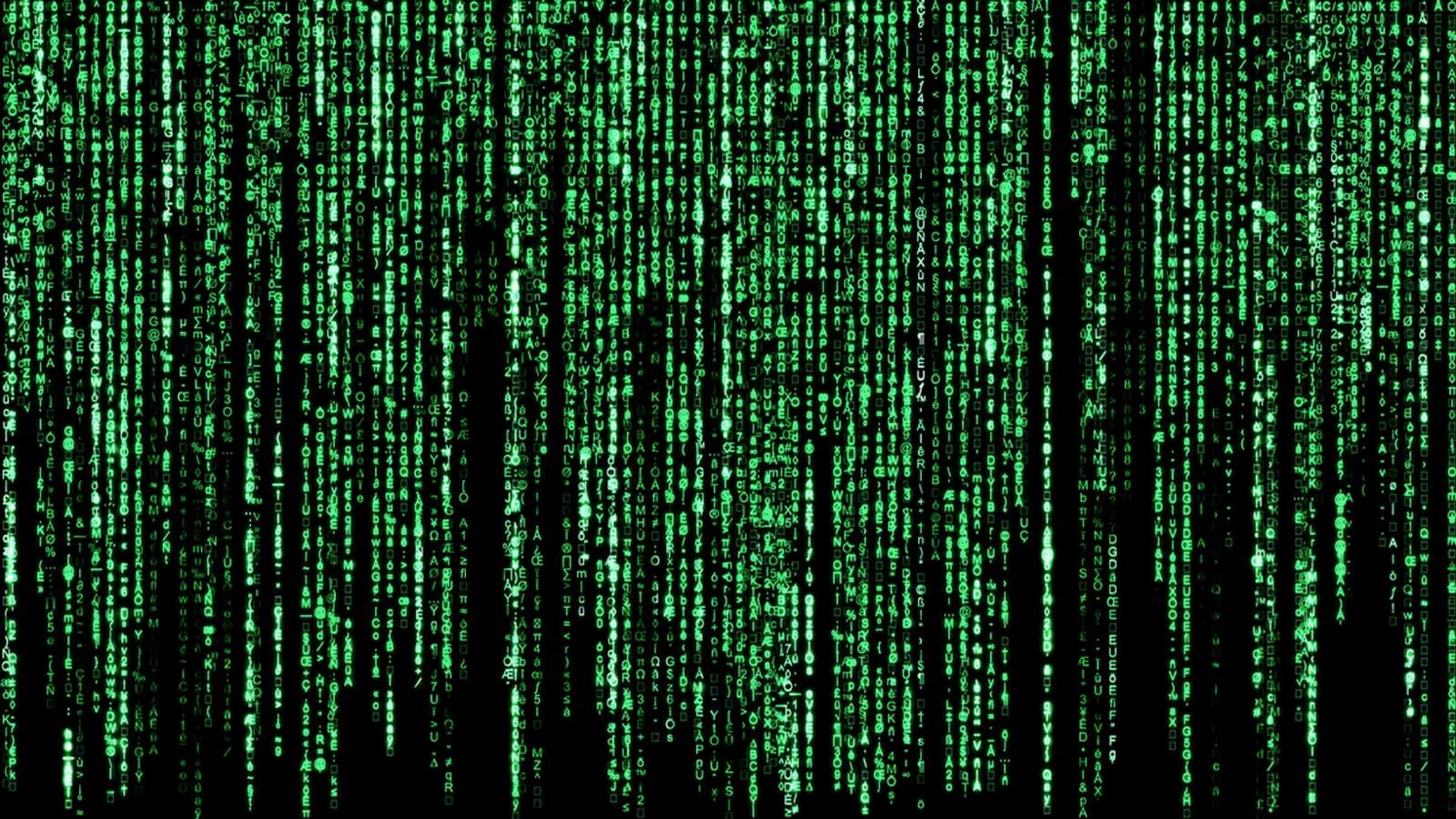


Von ARPANET - ARPANET, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=54039329

Erfindung des World Wide Web

Tim Berners-Lee – am CERN in Genf

Von Paul Clarke - Eigenes Werk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=37435469




A WERNER HERZOG FILM
LO AND BEHOLD
REVERIES OF THE CONNECTED WORLD

Einführung

Definition und Relevanz von Cyber Security

Was verstehen Sie unter Cyber Security

Definition von Cyber Security

- Cyber Security, auch als IT-Sicherheit oder Computersicherheit bekannt, bezieht sich auf den Schutz von Computersystemen und Netzwerken vor Diebstahl oder Beschädigung ihrer Hardware, Software oder elektronischen Daten sowie vor Störungen oder Missbrauch der bereitgestellten Dienste.
- In einem erweiterten Kontext schützt Cyber Security auch digitale Assets und Daten vor Diebstahl, Kompromittierung und unautorisiertem Zugriff.

Bedeutung von Cyber Security

- Insgesamt ermöglicht Cyber Security sowohl Unternehmen als auch Einzelpersonen, die Vorteile des Internets und der digitalen Technologie sicher zu nutzen, indem sie die Risiken von Datenschutzverletzungen, Datendiebstahl und anderen Cyber-Bedrohungen minimiert.
- Es ist ein ständig sich entwickelndes Feld, das sich an die sich ändernde Landschaft von Cyber-Bedrohungen und -technologien anpasst.

Bedeutung von Cyber Security

1. **Schutz von Geschäftsdaten**: Ein Hauptanliegen jedes Unternehmens ist es, die Integrität und Vertraulichkeit seiner Daten zu bewahren. Cyber Security stellt sicher, dass geschäftskritische Informationen vor externen und internen Bedrohungen geschützt sind.
2. **Bewahrung der Verbraucherinformationen**: Für viele Organisationen ist es von entscheidender Bedeutung, die Daten ihrer Kunden zu schützen. Datenlecks können zu massiven Vertrauensverlusten führen und haben finanzielle und rechtliche Konsequenzen.
3. **Sicherung der IT-Infrastruktur**: Ein stabiler Geschäftsbetrieb erfordert eine robuste IT-Infrastruktur. Cyber Security sorgt dafür, dass Netzwerke, Server und andere kritische Infrastrukturen vor Angriffen und Ausfällen geschützt sind.
4. **Verhinderung von Business Disruption**: Cyberangriffe können zu erheblichen Betriebsunterbrechungen führen. Dies kann zu direkten finanziellen Verlusten, Reputationsverlust und rechtlichen Konsequenzen führen.

Bedeutung von Cyber Security

5. **Einhaltung von Vorschriften**: In vielen Branchen und Ländern gibt es Vorschriften und Gesetze zum Schutz von Daten. Cyber Security gewährleistet die Einhaltung dieser Bestimmungen und vermeidet so potenzielle Strafen und rechtliche Konsequenzen.
6. **Schutz gegen fortgeschrittene Bedrohungen**: Mit der technologischen Entwicklung werden auch Cyberbedrohungen immer raffinierter. Cyber Security entwickelt sich kontinuierlich weiter, um Unternehmen vor diesen fortgeschrittenen Bedrohungen zu schützen.
7. **Förderung des Vertrauens in die digitale Transformation**: Viele Unternehmen setzen auf digitale Transformation, um wettbewerbsfähig zu bleiben. Ein solider Cyber-Security-Rahmen stellt sicher, dass diese Transformation sicher und reibungslos erfolgt.

Überblick

- ✓ **Grundlagen** und Entstehung vom World Wide Web
- ✓ **Einführung** in Cyber Security

- **Entwicklung** von Cyber Security Vorfällen
- **Massnahmen**
- Abschluss und Empfehlung
- Fragen und Antworten

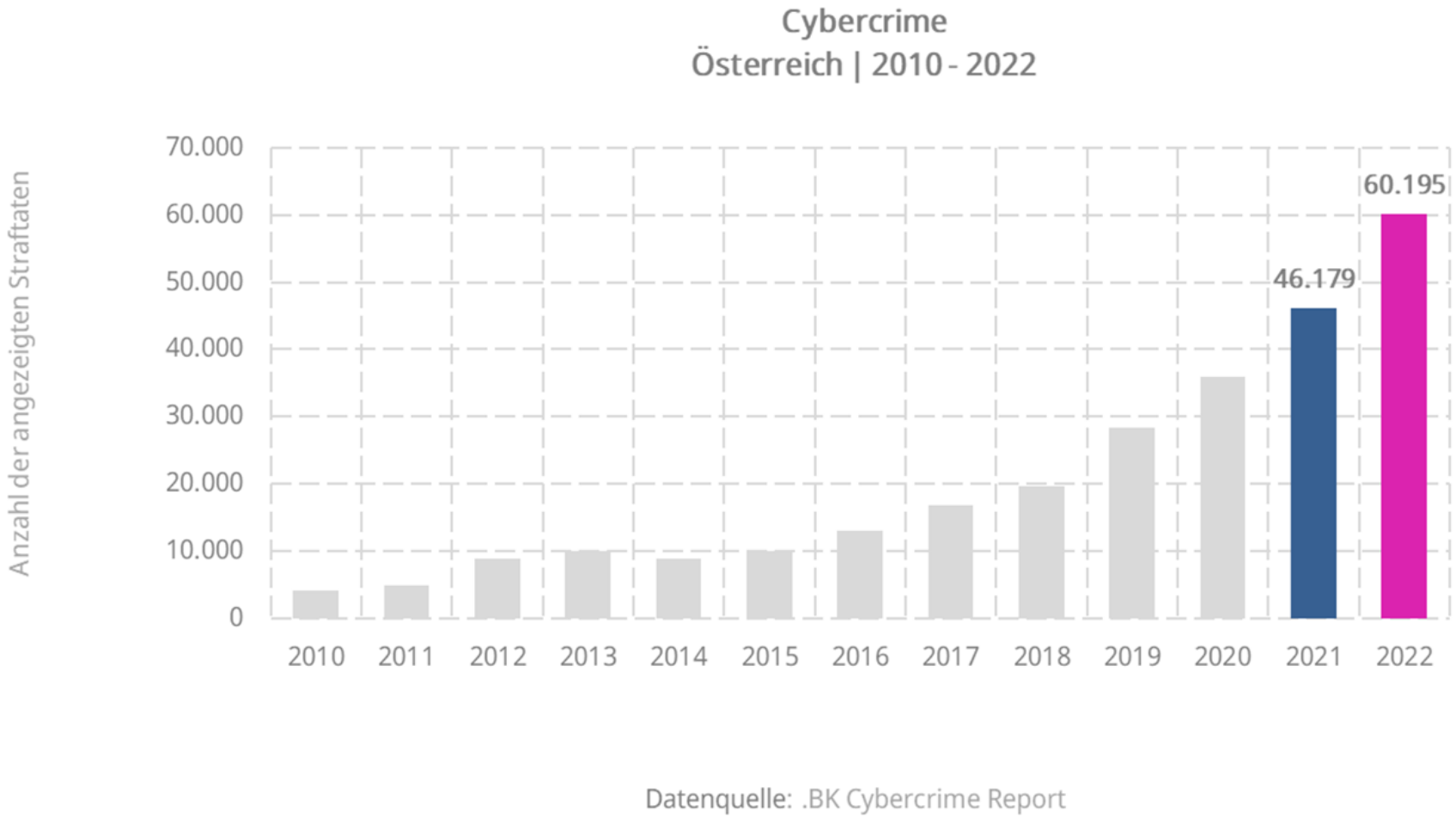
Entwicklung

Entwicklung und Arten von Vorfällen

Zunahme von Angriffen

- Es wurde allgemein beobachtet, dass die Anzahl der Cyberangriffe insgesamt zugenommen hat
- Mittelständische Unternehmen sind davon nicht ausgenommen. Ein Grund dafür ist, dass Cyberkriminelle festgestellt haben, dass mittelständische Unternehmen oft weniger fortgeschrittene Sicherheitssysteme haben als grosse Konzerne, sie aber immer noch wertvolle Daten besitzen.

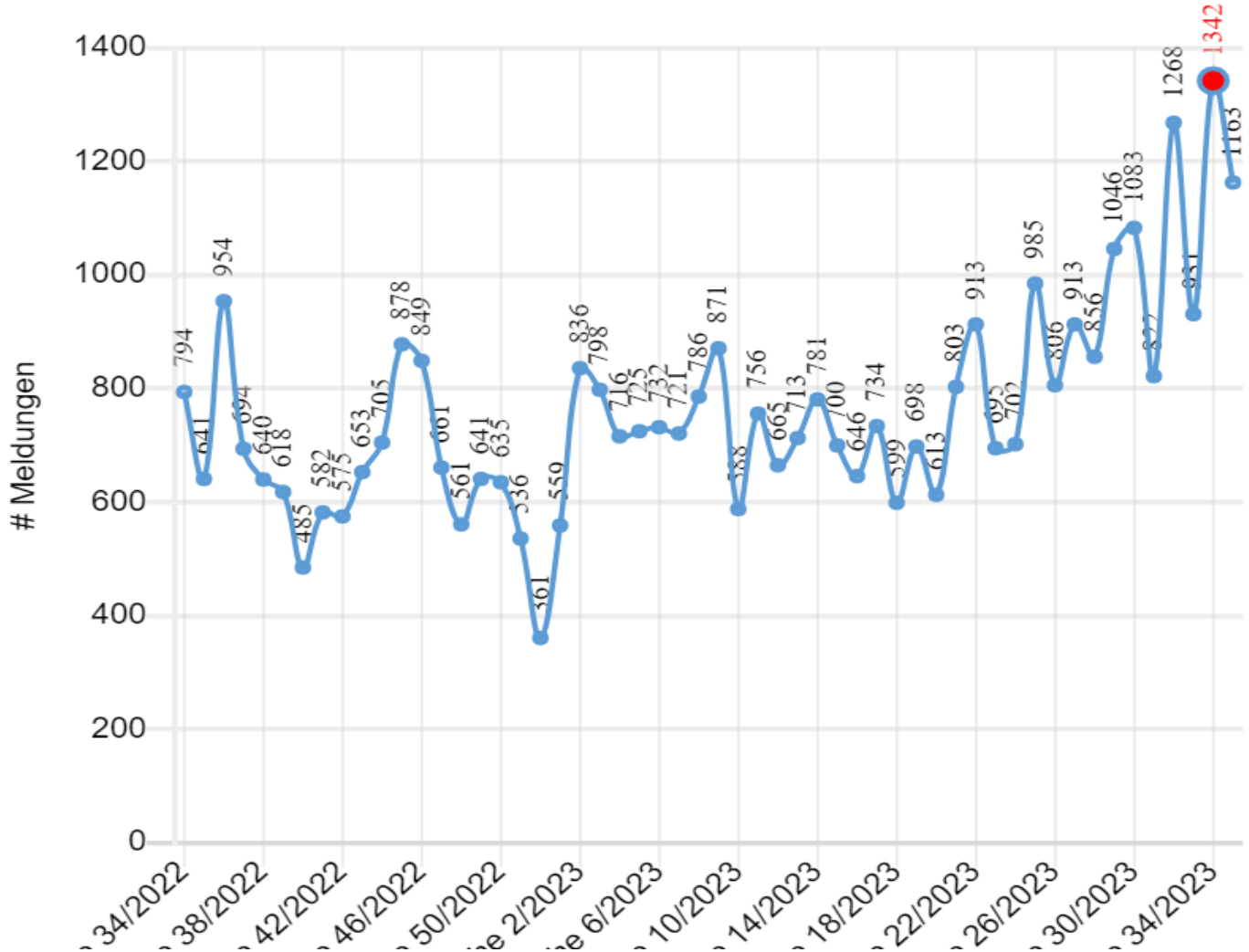
Entwicklung angezeigter Straftaten im Bereich Cyber



A-SIT Zentrum für sichere Informationstechnologie – Austria - Mai 2023

Meldungen pro Woche beim NCSC

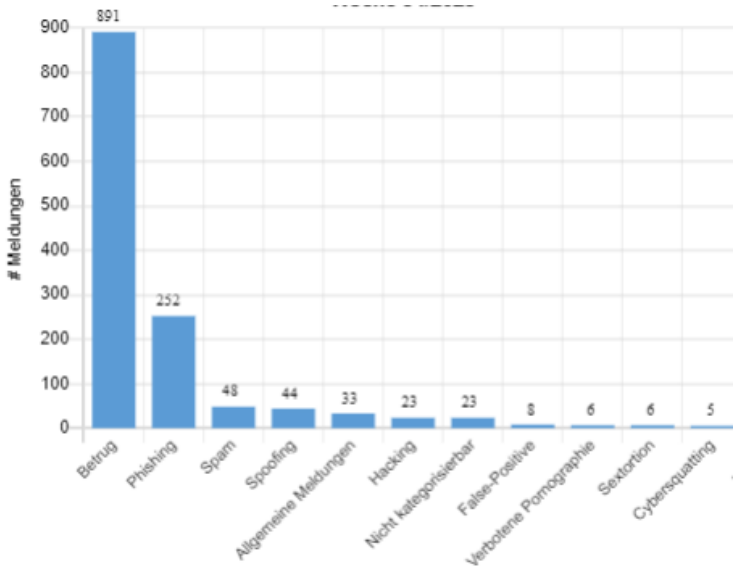
- Kontinuierliche Zunahme der beim NCSC gemeldeten Cyber Vorfälle im Verlauf vom vergangenen Jahr

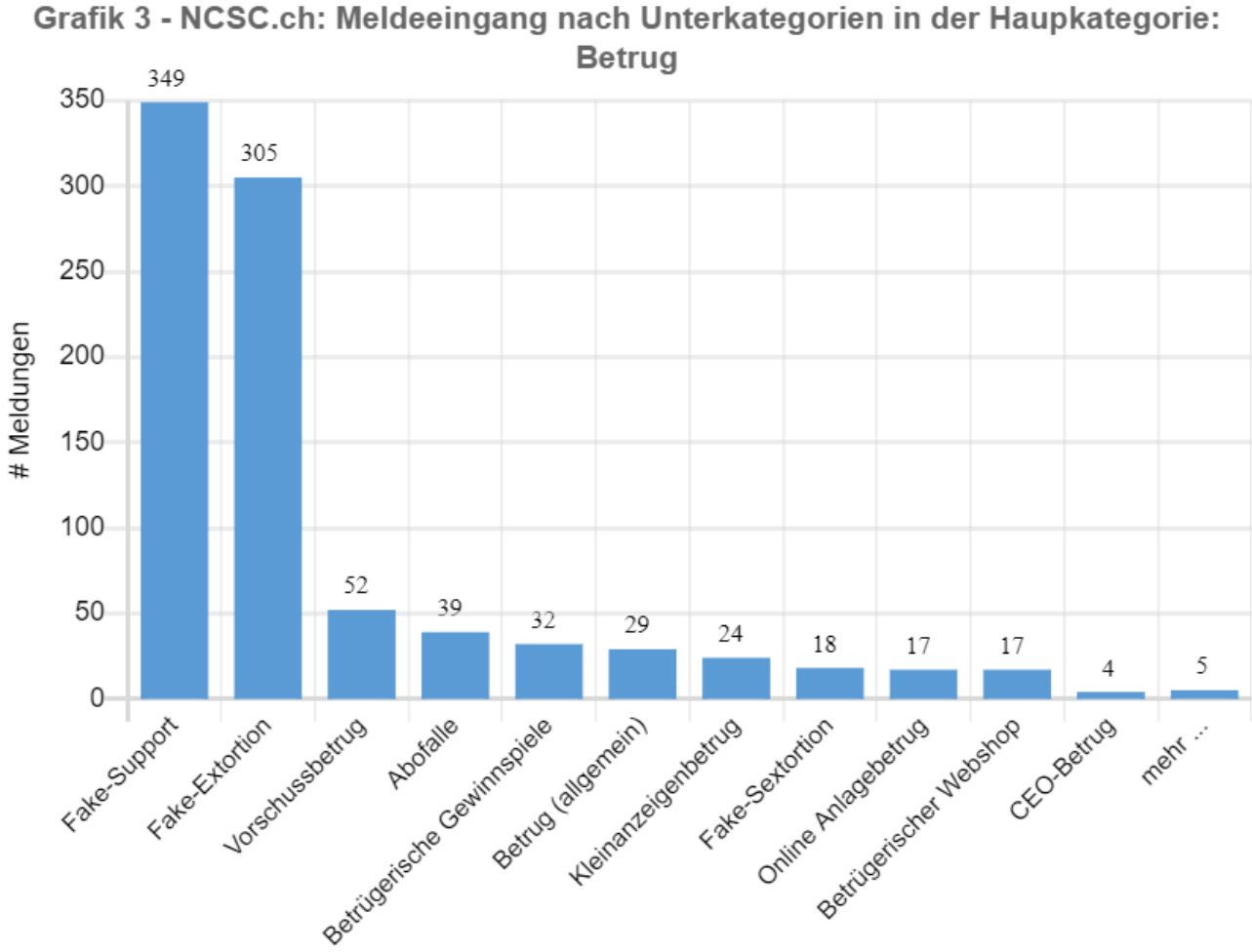


Gemeldete Betrugsfälle in KW 34/2023

- In KW34/2023 wurden 1342 Vorfälle gemeldet, davon

  891 Kategorie Betrug
  252 Kategorie Phishing





Welches sind die wesentlichen Angriffsvektoren ?

Die 8 wichtigsten Angriffsvektoren

Ransomware Angriffe

- **Beschreibung**: Malware, die Daten des Opfers verschlüsselt und ein Lösegeld für den Entschlüsselungscode verlangt.
- **Auswirkungen**:
  - Datenverlust, wenn kein Backup vorhanden ist oder das Backup ebenfalls kompromittiert wurde
  - Betriebsunterbrechung
  - Finanzielle Verluste durch Lösegeldzahlungen
  - Reputationsverlust

Phishing & Spearphising

- **Beschreibung**: Betrügerische E-Mail-Angriffe, die den Empfänger dazu verleiten sollen, vertrauliche Daten preiszugeben oder Malware herunterzuladen.
- **Auswirkungen**:
  - Diebstahl von Anmeldeinformationen.
  - Finanzieller Betrug.
  - Installation von Malware auf dem System des Opfers.

Man-in-the-Middle Angriffe

- **Beschreibung**: Ein Angreifer fängt Kommunikation zwischen zwei Parteien ab und kann diese einsehen, möglicherweise manipulieren.
- **Auswirkungen**:
  - Datenverlust
  - Datenschutzverletzungen
  - Fehlinformation oder Manipulation von Transaktionen

Distributed Denials-of-Service (DDoS)

- **Beschreibung**: Versuche, einen Server oder ein Netzwerk zu überfluten und dessen regulären Betrieb zu stören.
- **Auswirkungen**:
  - Betriebsunterbrechung
  - Reputationsverlust
  - Potenzielle finanzielle Verluste durch Unterbrechung von Online-Diensten

Drive-by-Downloads

- **Beschreibung**: Ein Angreifer nutzt ein schädliches Skript, um Malware auf das Gerät eines Benutzers herunterzuladen, oft ohne das Wissen / Bemerken des Benutzers.
- **Auswirkungen**:
  - Installation von Malware, Spyware oder Ransomware
  - Datenverlust oder -diebstahl
  - Systemkompromittierung

SQL-Injection

- **Beschreibung**: Ein Angreifer nutzt schlecht geschützte Webanwendungen, um schädliche SQL-Codes auszuführen und so auf Datenbanken zuzugreifen.
- **Auswirkungen**:
  - Datenverlust oder -diebstahl
  - Manipulation von Datenbankdaten
  - Verlust der Datenintegrität

Zero-Day-Exploits

- **Beschreibung**: Angriffe, die Schwachstellen in Software oder Hardware ausnutzen, bevor der Entwickler eine Lösung oder ein Patch herausbringen kann.
- **Auswirkungen**:
  - Unautorisierte Systemzugriffe
  - Datenverlust oder -diebstahl
  - Installation von Malware

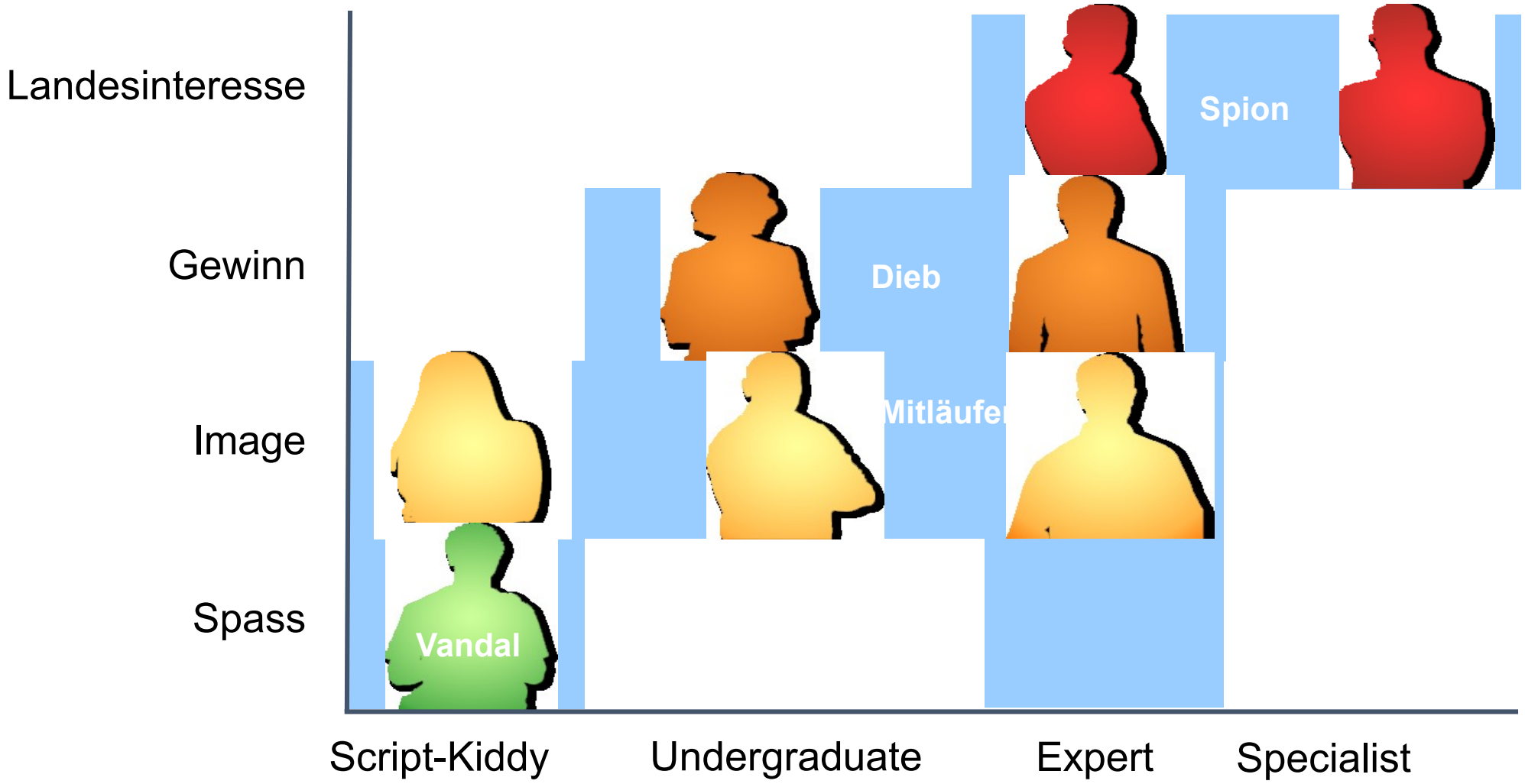
Insider-Threats

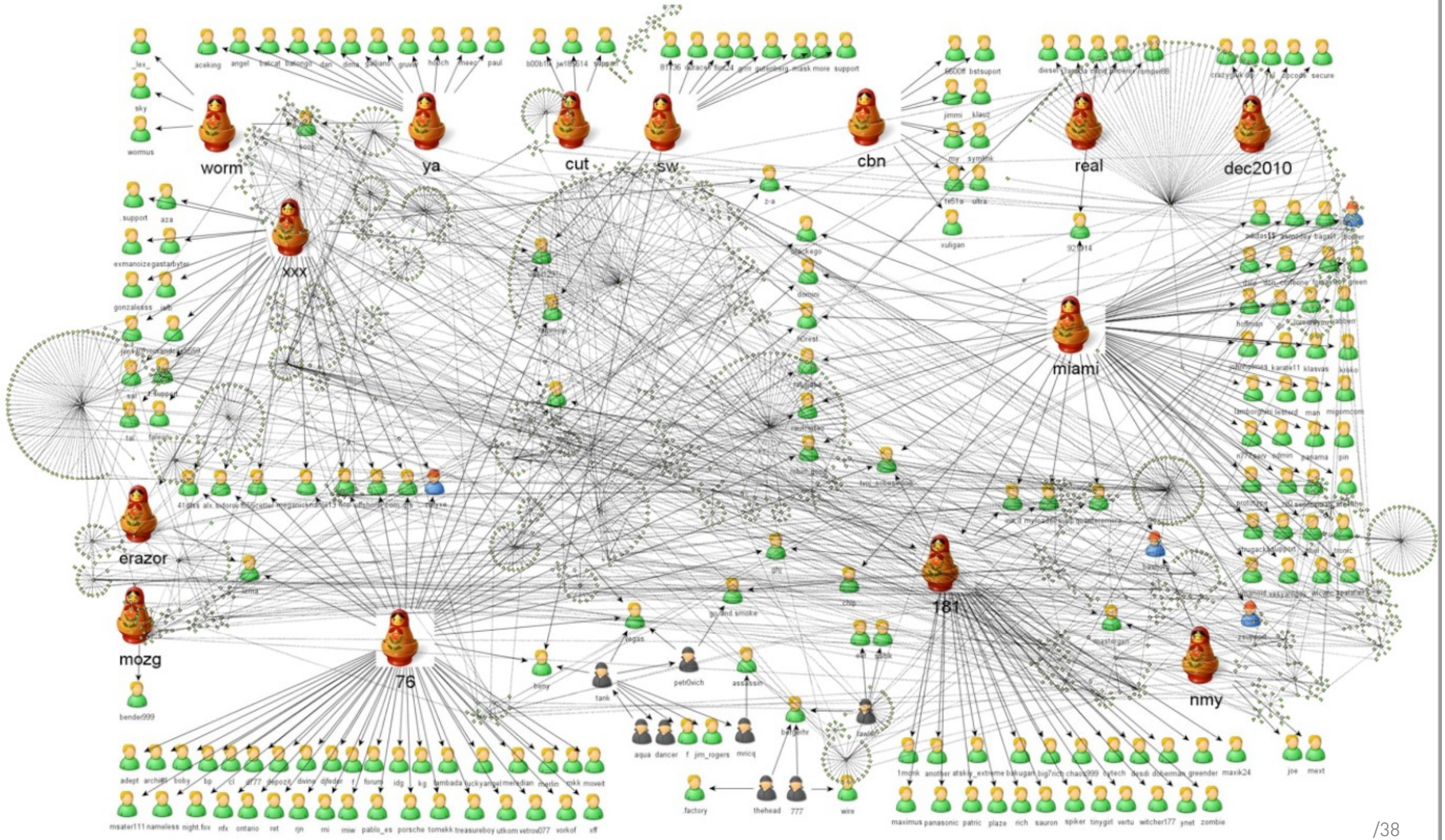
- **Beschreibung**: Bedrohungen, die von Personen innerhalb der Organisation stammen, z.B. von Mitarbeitern, ehemaligen Mitarbeitern oder Geschäftspartnern.
- **Auswirkungen**:
  - Datenverlust oder -diebstahl
  - Betriebsunterbrechungen
  - Reputationsverlust

Derzeit grösste Risiken

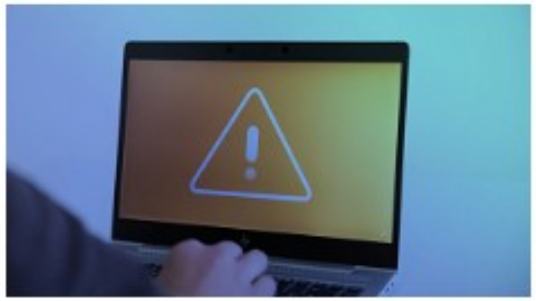
Bespiele und deren Auswirkungen

Bedrohungen – Wer bedroht uns




worm
ya
cut
sw
cbn
real
dec2010
xxx
miami
erazor
mozg
76
181
nmy

Cyberbedrohungen des aktuellen Monats



Gefälschte Drohmails von Behörden

Investmentbetrug

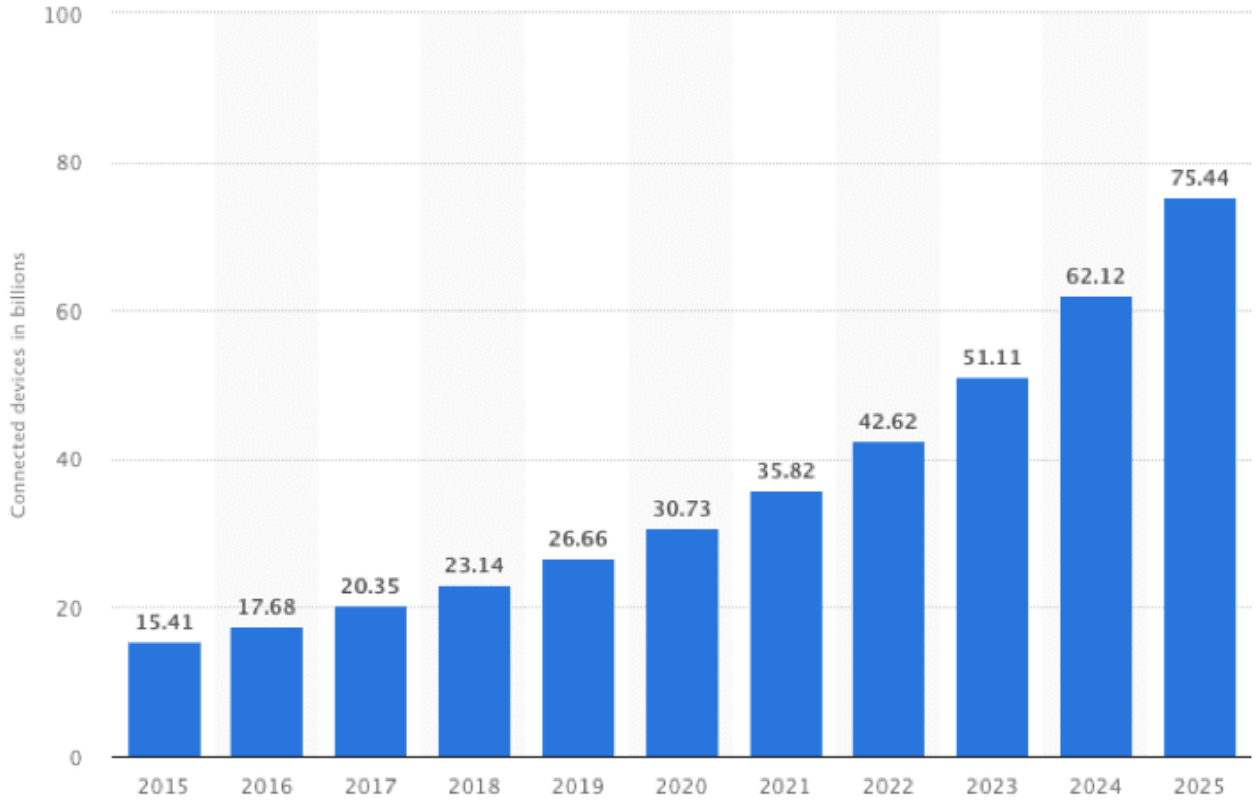
Ransomware

Fake Sextortion

Quelle: Nationales Zentrum für Cyber Sicherheit der Schweiz NCSC - September 2023

Unsichere IoT Geräte

- Mit dem raschen Anstieg von IoT-Geräten, die oft unzureichend gesichert sind, gibt es immer mehr Eintrittspunkte für Angreifer.



Von Statista 2019

Von Netzwoche

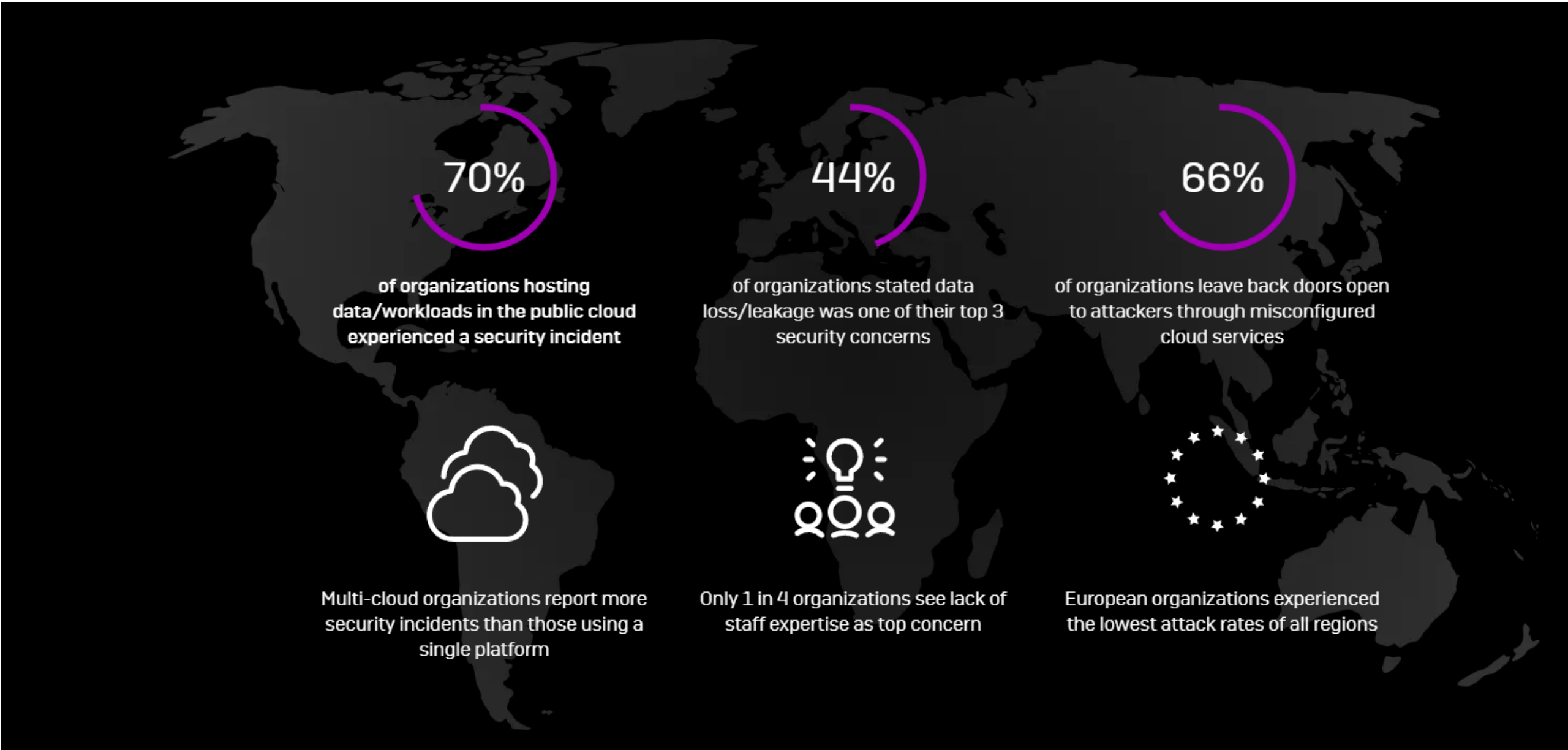
Cloud Sicherheitslücken

- Mit der weiteren Adoption von Cloud-Technologien sind Fehlkonfigurationen und unsichere Schnittstellen zu bedeutenden Bedrohungen für Daten in der Cloud geworden.

Von wisdomPlexus

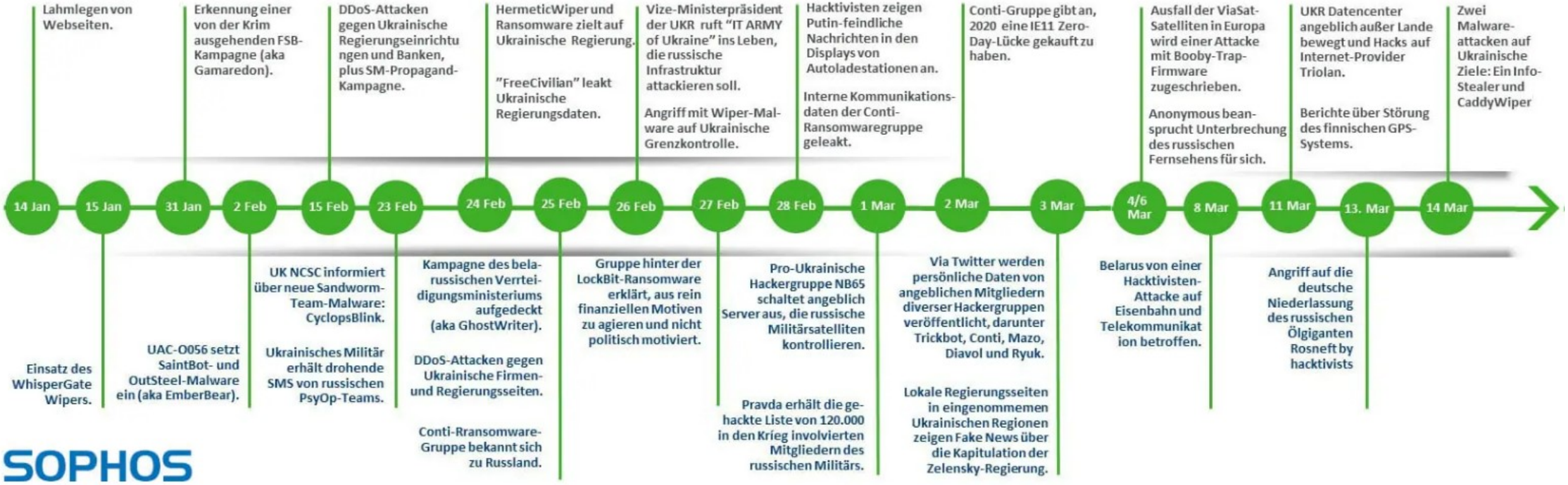
Cloud Security Status 2020 von SOPHOS

WEIHRICH INFORMATIK



Wachsende nationale Cyberangriffe

- Staaten oder staatsnahe Akteure nutzen zunehmend Cyberangriffe zu Spionage-, Sabotage- oder Einflusszwecken.



Bericht von Chester Wisniewski ist Principal Research Scientist bei Sophos 2022

Künstliche Intelligenz (KI)

- Während KI in der Cyber-Abwehr eine wachsende Rolle spielt, nutzen Angreifer sie auch, um Angriffe zu automatisieren, Malware zu mutieren und Sicherheitssysteme zu umgehen.

https://systag.com/ KI basierte Cyber Abwehr vs. Pattern basierte Antiviruslösung

Überblick

- ✓ **Grundlagen** und Entstehung des World Wide Web
- ✓ **Einführung** in Cyber Security
- ✓ **Entwicklung** von Cyber Security Vorfällen

- **Massnahmen**
- Abschluss und Empfehlung
- Fragen und Antworten

WEIHRICH
INFORMATIK

Massnahmen

Empfehlungen zur Verbesserung der Cyber Sicherheit für KMU

Sicherheitsmassnahmen sind erforderlich

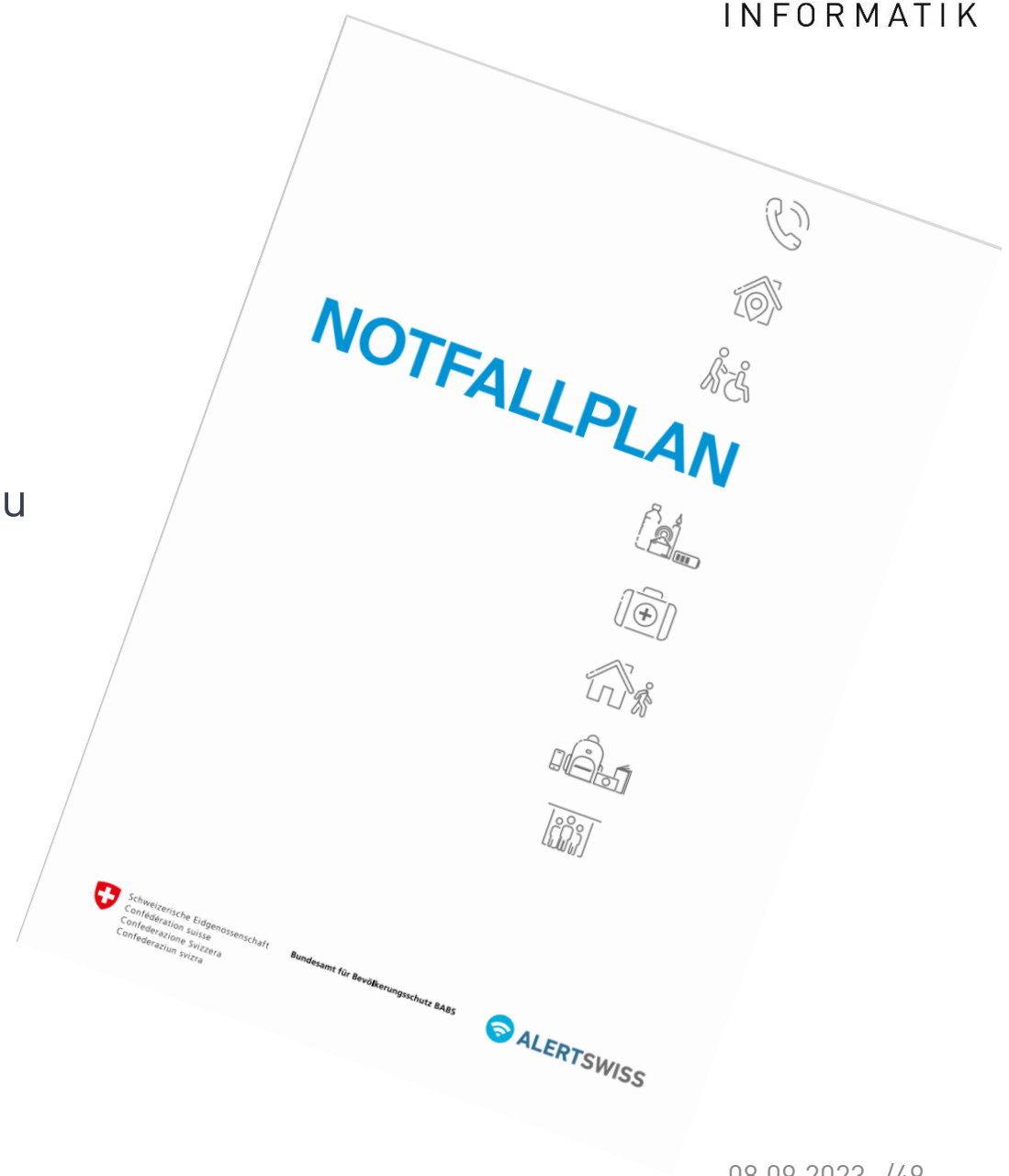
- Diese Angriffe und ihre potenziellen Auswirkungen unterstreichen die Notwendigkeit für Unternehmen, proaktive Sicherheitsmassnahmen zu implementieren und ständig wachsam zu sein. Es ist auch wichtig, Mitarbeiter regelmässig zu schulen und auf dem neuesten Stand der aktuellen Bedrohungen und besten Sicherheitspraktiken zu halten.

➢ IT Security ist Chefsache

Mangelnde Vorbereitung

- Studien und Umfragen haben gezeigt, dass viele mittelständische Unternehmen sich nicht ausreichend auf mögliche Cyberangriffe vorbereitet fühlen oder nicht über die notwendigen Ressourcen verfügen, um ihre Systeme und Daten ausreichend zu schützen.

Erstellen Sie einen Notfallplan



Organisatorische Empfehlungen

- Erstellen Sie einen Plan
  - Notfallplan zur Begrenzung von Schäden
- Schaffen Sie Wissen und Bewusstsein
  - Anwendungsschulung
  - Sicherheitsschulung
- Reagieren Sie auf Änderungen
- Werden Sie skeptisch

Risikobewertung

Kriterien für eine Risikomatrix

Ausmaß	×	Eintrittswahr-scheinlichkeit	=	Auswirkungen
Unwesentlich		Sehr wahrscheinlich		Niedrig
Gering		Wahrscheinlich		Mittel
Mittel		Möglich		Hoch
Hoch		Unwahrscheinlich		
Kritisch		Sehr unwahrscheinlich		

https://asana.com/

IKT-Minimalstandard (admin.ch)

Mitarbeiter Schulung

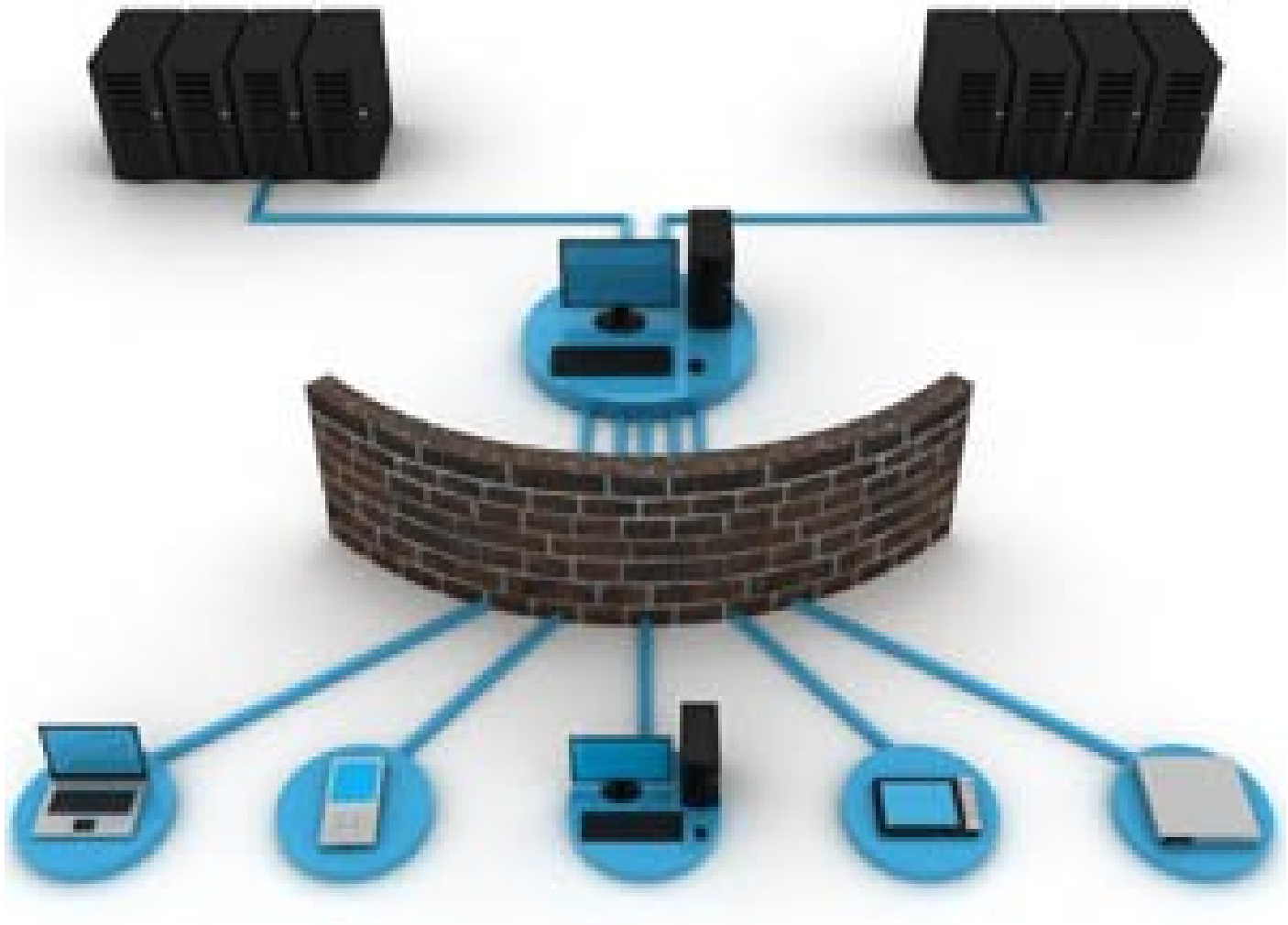
- Die meisten Sicherheitsvorfälle beginnen mit **menschlichen Fehlern**, sei es durch das Klicken auf schädliche Links oder den Download von infizierten Anhängen.
- Regelmässige Schulungen können Mitarbeiter für Sicherheitsrisiken sensibilisieren und ihnen beibringen, sicherheitsbewusstes Verhalten an den Tag zu legen.

Zeitgemässer Betrieb und Unterhalt

Quelle: HPE Innovation Circle September 2018

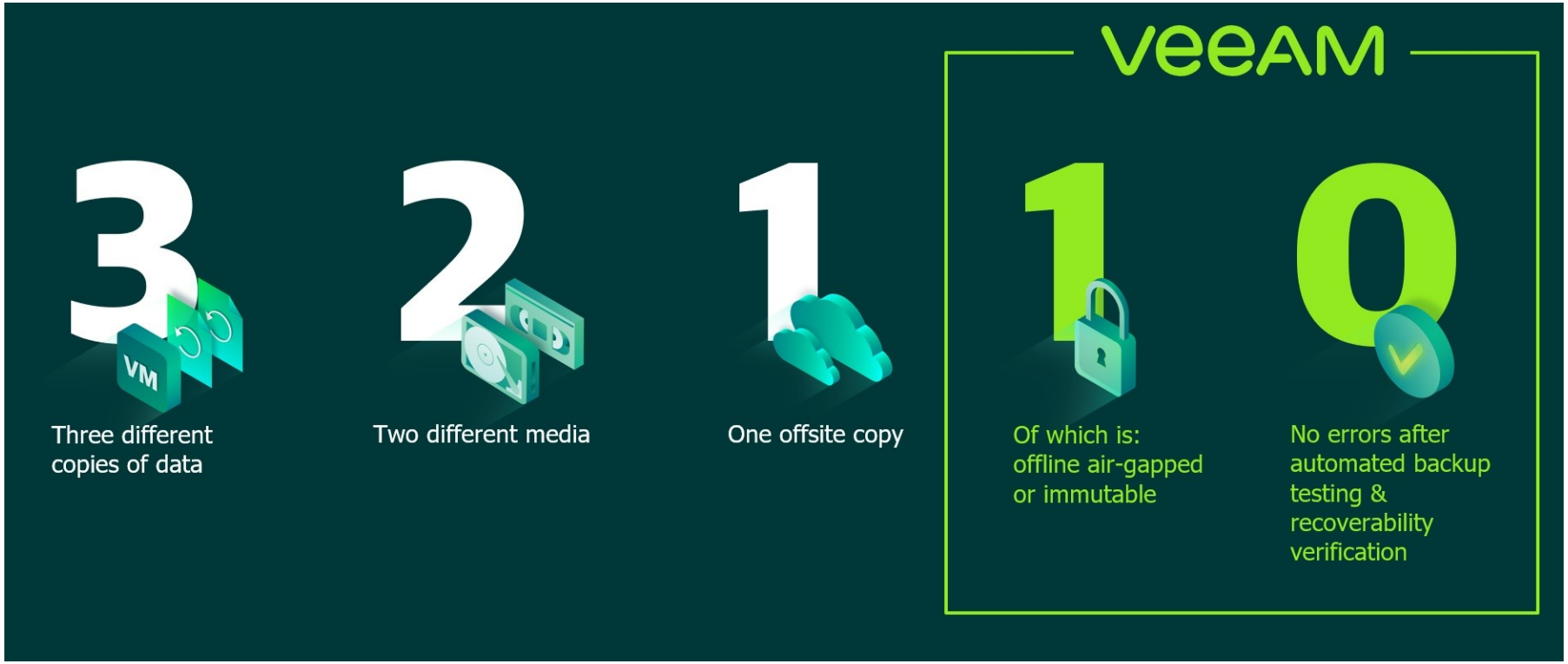
Technische Empfehlungen

- Werden Sie aktiv
  - Interne Systemanalyse
  - Externe Systemanalyse
- Machen Sie Ihre Systeme sicher
  - Umfassende Systemoptimierung
  - Regelmässige Aktualisierung
    - Ihrer Netzwerkinfrastruktur
    - Ihrer Server und PC Infrastruktur
    - Ihrer Anwendungen
- Verwenden Sie eigene Geräte

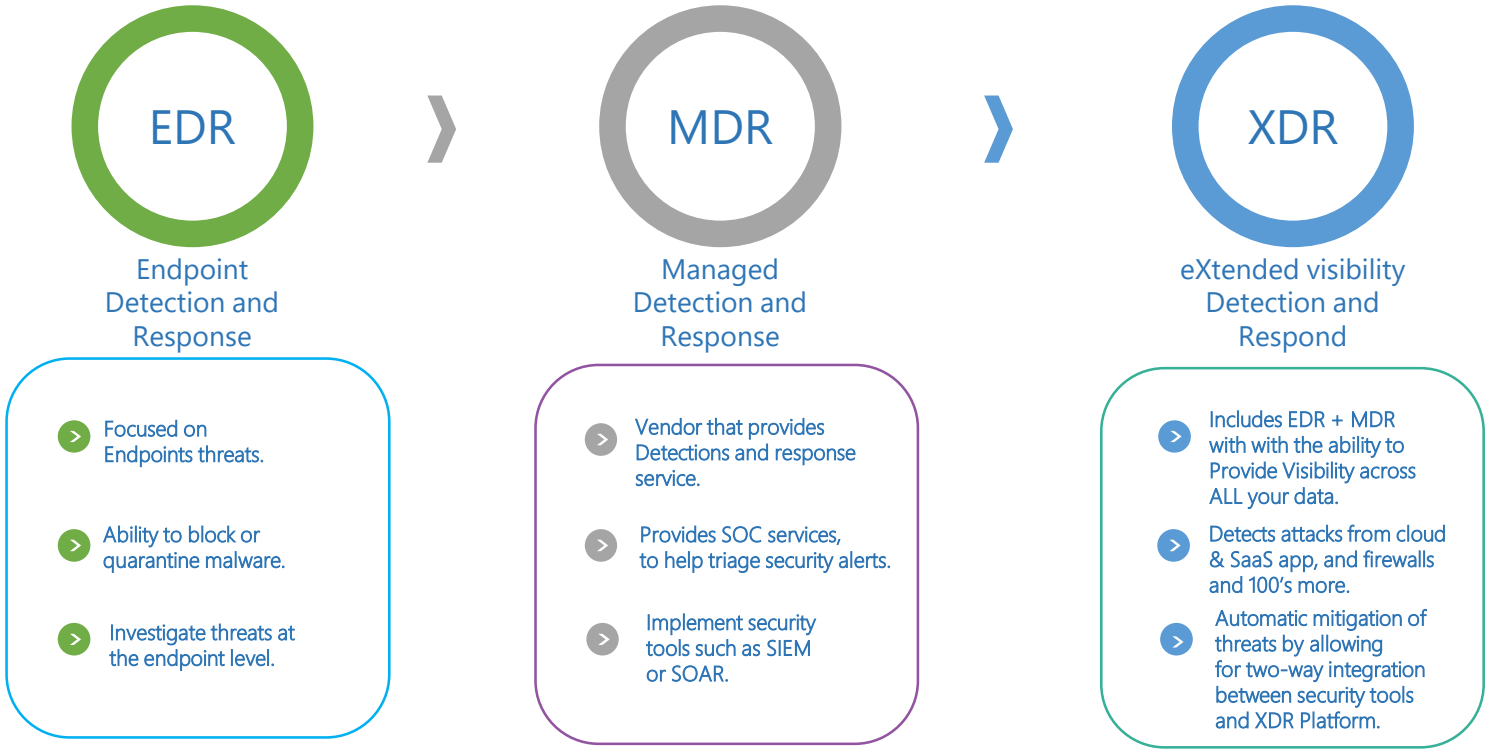


Backup Strategien

- Datensicherungen schützen vor Datenverlust, sei es durch Hardwareausfälle, Cyberangriffe wie Ransomware oder menschliche Fehler.
- Regelmässige Back-ups, die sowohl lokal als auch remote gespeichert werden. Die 3-2-1-Regel (drei Kopien der Daten, auf zwei verschiedenen Medien, eine davon extern) ist ein gängiger Ansatz.

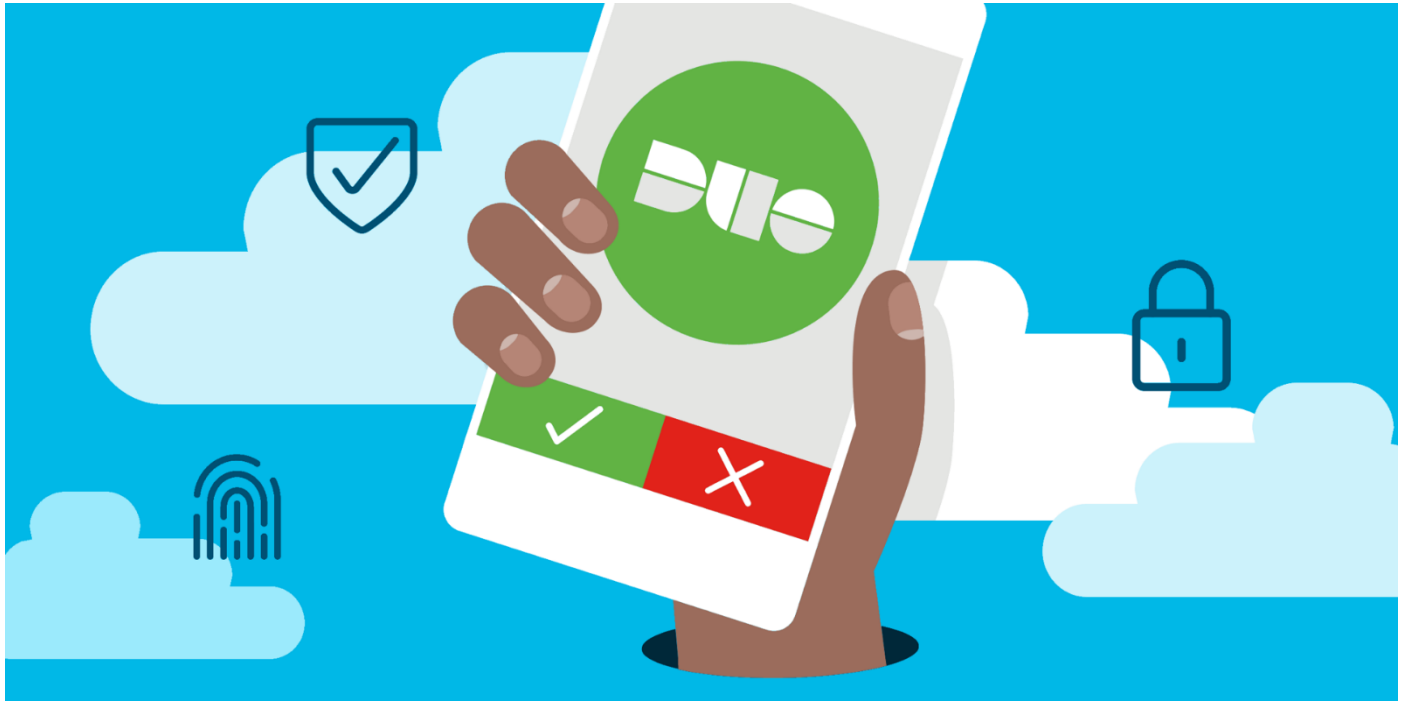


EDR vs MDR vs XDR



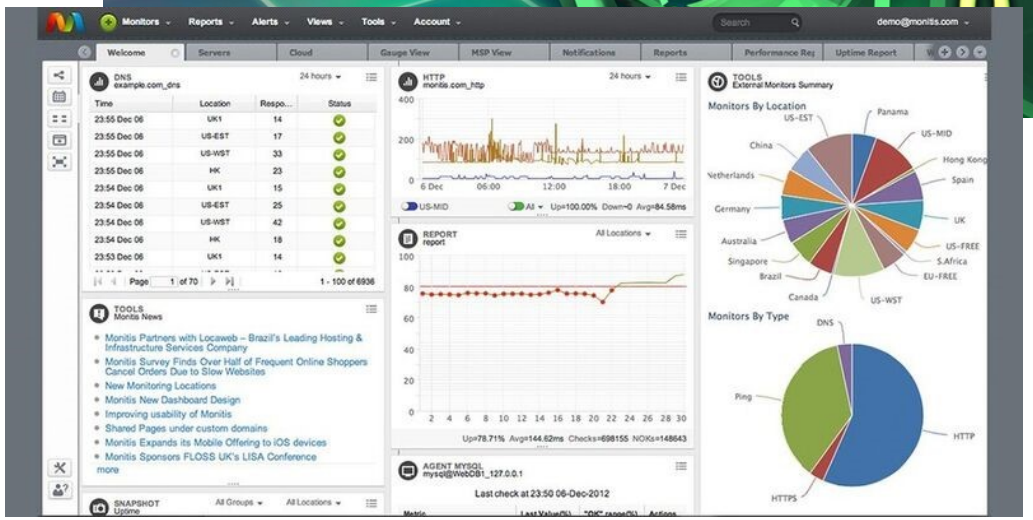
Mehrfaktor Authentifizierung

- Zusätzlich zu Benutzernamen und Passwort erfordert dies eine zweite Form der Identifikation, z. B. einen Code von einem Authentifizierungs-App oder einen Fingerabdruck.
- Dies stellt sicher, dass selbst wenn Passwörter kompromittiert werden, Angreifer keinen Zugang zu den Konten erhalten.



Modernes Netzwerk

- Dabei wird das Netzwerk in verschiedene Segmente unterteilt, so dass, falls ein Segment kompromittiert wird, der Angreifer nicht automatisch Zugang zu allen Bereichen des Netzwerks hat.
- Dies kann dazu beitragen, die Ausbreitung von Malware zu verhindern und den Schaden bei einem Sicherheitsvorfall zu begrenzen.
- **Netzwerkmonitoring** ist der Schlüsselfaktor für den Erfolg



https://www.ip-insider.de/

Sichere Passwörter

- Verwenden Sie sichere Passwörter
- Speichern und verwalten Sie Ihre Passwörter sicher
- Nutzen Sie moderne Werkzeuge zur sicheren und effizienten Anwendung von Passwörtern

Passwörter zentral, sicher und einfach aufbewahren

WEIHRICH INFORMATIK

In der immer weiter digitalisierten Welt verfügt jede Person über eine immer grösser werdende Zahl an Benutzerkonten: Zugangsdaten mit Benutzernamen und Passwort für den Arbeitsplatz, den privaten PC, das eBanking, den Internet-Shop oder die Vereinshomepage. Häufig nutzen Anwenderinnen und Anwender für diese Benutzerkonten identische Zugangsdaten. Diese Tatsache führt unweigerlich dazu, dass einem Angreifer bei der Offenlegung nur eines Benutzerkontos praktisch alle Türen offenstehen. Auch werden Passwörter immer noch häufig in einfachen Word- oder Excel-Dateien oder als Outlook-Notizen unverschlüsselt abgelegt. Bei Ferienvertretungen, oder wenn andere Personen dieselben Zugangsdaten verwenden, werden diese sensiblen Informationen als Kopie weitergegeben.

Diese unbefriedigende Situation kann grundsätzlich dadurch wesentlich verbessert werden, wenn für jedes Benutzerkonto ein individuelles Password festgelegt wird. Jedoch ist dies oft nur schwer möglich, da bei der Vielzahl an Benutzerkonten ohne technische Hilfsmittel leicht der Überblick verloren geht. Mit einem modernen Passwortmanager kann mittels des integrierten Passwortgenerators zudem sichergestellt werden, dass die verwendeten Passwörter heutigen Anforderungen entsprechen und einzigartig sind.

Weihrich Informatik bietet Ihnen zur modernen Passwortverwaltung zwei Optionen an. Das «Password Depot» eignet sich am besten für Geschäftsumgebungen, bei denen ein zentral über das Active Directory zur Verfügung steht und die Nutzer sich lokales Active Directory anmelden. Ebenso eignet sich das «Password Depot» hervorragend für Remote Desktop Umgebungen (RDP) und für die Regelung der Zugriffsmöglichkeiten über Sicherheitsgruppen. Alle Informationen sind zentral und verschlüsselt abgelegt, der Zugriff und Veränderungen werden protokolliert und der Zugang kann jederzeit und sehr individuell angepasst werden.

Für Unternehmen und Privatpersonen, welche nicht über eine zentrale Serverinfrastruktur verfügen, oder weit verteilt in Homeoffice Umgebungen arbeiten, eignet sich die cloudbasierte Lösung «Bitwarden» am besten. Der Zugriff auf die Passwörter ist weltweit von allen Geräten sowie webbasiert möglich.

Beide Lösungen garantieren eine sichere Verwaltung Ihrer Passwörter. Ihre Passwörter befinden sich niemals unverschlüsselt auf einem Server, die Entschlüsselung Ihrer Passwörter erfolgt immer lokal auf Ihrem Gerät.

	Password Depot		Bitwarden (Teams)
Datenhaltung	On-Prem Server		Cloud
Zugriff	Lokal (mit RDS)		weltweit
Verschlüsselung	AES-256 Bit		AES-256 Bit/Web
AD-Integration	✓		✓ (mit RDS)
2-FA	✓		✓
Benutzergruppen	✓		✓
Teilen im Team	✓		✓
2-FA im PW Manager	✓		✓
Benutzer-definierte Rollen	einschränkt		✓
Mobiler App Zugriff	✓		✓
Zeitlich beschr. Zugriff	✓		✓

© Weihrich Informatik GmbH Version 2023-09

Weihrich Informatik GmbH · Alleestrasse 20 · CH-8280 Kreuzlingen · Tel +41 (0)71 688 33 30 · Fax +41 (0)71 688 33 23 · info@weihrich.ch · www.weihrich.ch

Abschluss und Empfehlung

Seien Sie wachsam und vorbereitet

Unsere Empfehlung: Strategie

- Unternehmensstrategie
  - Unternehmensentwicklung und Tätigkeit ✓
  - Standorte und Leistungen ✓
  - Bedürfnisse und Arbeitsweise der Mitarbeitenden
- Strategie Fachapplikationen
  - Prüfung / Evaluation der geeigneten Fachapplikationen
- IT Strategie
  - Ausarbeitung einer auf die Unternehmung und deren Entwicklung abgestimmten IT Strategie
- Massnahmenplan
  - IKT Analyse und Standortbestimmung
  - IKT Massnahmen zur Optimierung von Betrieb und Unterhalt


Corporate Responsibility

Unsere Empfehlung: Modern Managed Workplace

- Klarsicht statt Blindflug

- Automatisierte Statistiken statt manueller Inventarlisten, proaktive Echtzeit-Überwachung statt (zu) später Reaktion, laufende System-Überwachung und damit eine höhere Sicherheit – geeignete «Managed Workplace Lösungen» gibt es heute auch für KMU.


TRANSPARENZ


MERCI

Fragen und Antworten

Sie haben noch Fragen ?

So erreichen Sie uns

Bürozeiten
Mo – Fr
8-12 / 13-17 Uhr

Bei technischen Anliegen
+41 (0)71 677 13 30

Bei allgemeinen Anliegen
+41 (0)71 688 33 30

Bei technischen Anliegen
helpdesk@weihrich.ch

Bei allgemeinen Anliegen
info@weihrich.ch

Weihrich Informatik GmbH
Alleestrasse 20
8280 Kreuzlingen

MMWP by WEIT – PLATIN

	Anti-Virus		Dienstleistungen				
	EDR	XDR	Easy Remote Management	Monitoring	Asset Management	Betriebssystem Updates	Advanced Software Mgt.
	integrierter Virenschutz	*Virenschutz mit XDR Technologie und Zugang zu SOC*	*für einfachen und sicheren Support*	*für das Erkennen von Auslastungs-Trends*	*für die Dokumentation aller Komponenten Ihrer IT*	*für stabile und sichere Systeme*	*für zusätzliche Sicherheit bei Dritt-Software*
Bronze	Dritt-Produkt		✓				
Bronze +	✓		✓				
Bronze XDR		✓	✓				
Silber	Dritt-Produkt		✓	✓	✓		
Silber +	✓		✓	✓	✓		
Silber XDR		✓	✓	✓	✓		
Gold	Dritt-Produkt		✓	✓	✓	✓	
Gold +	✓		✓	✓	✓	✓	
Gold XDR		✓	✓	✓	✓	✓	
Platin	Dritt-Produkt		✓	✓	✓	✓	✓
Platin +	✓		✓	✓	✓	✓	✓
Platin XDR		✓	✓	✓	✓	✓	✓

Unsere Service-Pakete

Strategie-Paket

Grobvorschlag für mittel- und langfristige Informatik-Strategie basierend auf einer Standortbestimmung

Investment-Paket

Investitionsplanung zur Optimierung der IT-Gesamtkosten

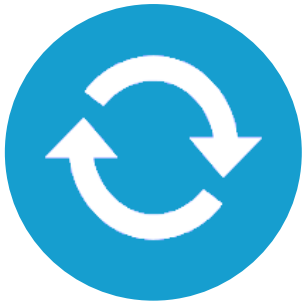
Security-Paket

Vorschlag Massnahmenkatalog zur Erhöhung der System-Sicherheit

Unsere Service-Pakete

Komm-Paket

Analyse der Kommunikationskosten, Aufzeigen von Verbesserungen und Sparpotenzial



Update-Paket

Wir überprüfen Ihre EDV-Systeme auf notwendige Aktualisierungen und unterbreiten Ihnen einen Massnahmenplan

Data-Paket

Wir verschaffen uns einen Überblick über Ihre Dokumentenverwaltung und unterbreiten Ihnen einen Grobvorschlag, wie Sie die Effizienz Ihrer Unternehmung steigern können

Referenzen

Seit 2013 leistet das Team von Weihrich Informatik GmbH einen professionellen Support für unsere vielen Nutzer. Mit dem Neubau und der Renovation der Häuser im Jahr 2018 haben wir grundlegende modernste Neuinstallationen sowie eine Neuorganisation des Netzwerkes mit Anbindung von Servern, Backup, WLAN und Einbindung an topaktuelle Alarm- und Telefonieanwendungen erhalten. Wir zählen weiterhin auf die schlanke Koordination und gute Kooperation vom Profi zu uns als Anwender im Gesundheitswesen. Vielen Dank.

Mirjam Brühwiler, Geschäftsleiterin
Abendfrieden, Wohnen & Pflege, Kreuzlingen

Referenzen

Als wachsendes Unternehmen bieten wir unseren Kunden Dienstleistungen nach Mass im Bereich Projektentwicklung, Planung, Ausführung bis zur Ausstattung von Wohnbauten, Hotel/Resorts und Infrastrukturbauten. Für unsere mehr als 100 Mitarbeitenden sind Schnelligkeit und Genauigkeit genauso wichtig wie Effizienz und Zuverlässigkeit. Weihrich Informatik als langjähriger Partner sorgt dafür, dass wir dazu auf eine moderne EDV-Infrastruktur an mehreren Standorten und sichere, hochverfügbare Systeme zurückgreifen können. Auf Geschäftsleitungsebene schätzen wir den Austausch auf Augenhöhe.

Hans Peter Hoffmann, Mitglied der Geschäftsleitung und des Verwaltungsrats
Baulink AG, Davos

Referenzen

Firmenübernahme, Kompletterneuerung EDV, Kompletterneuerung Telefonie: Der Fokus lag auf einer an unseren Bedürfnissen und Prozessen aus-gerichteten, kosteneffizienten und nachhaltigen Lösung. Die Planung und Umsetzung übernahm Weihrich Informatik. Ein Entscheid, den wir nicht bereut haben.

Peter Gsell, Inhaber
Gsell Fenster GmbH, Romanshorn