Ist Ihr KMU sicher?

Herzlich Willkommen

IT Sicherheit ⋆ ⋆ ⋆
eine Herausforderung für KMU

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Der Mythos: IT Sicherheit = eine Herausforderung für KMU

zu teuer

zu komplex

mühsam

keine Priorität

kein unmittelbarer Nutzen

zeitaufwändig

zu schnell-lebig

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

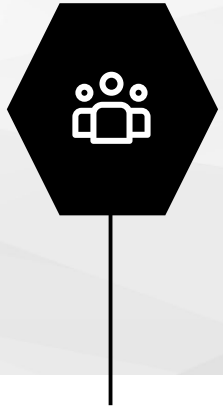
Der AGVS setzt sich dafür ein, seine Mitglieder im Bereich IT-Sicherheit aufzuklären.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Cyberbedrohung
Max Klaus,
stv. Leiter Operative Cybersicherheit,
NCSC

So schützen Sie Ihr KMU
Yves Arnosti,
IT Experte,
Swisscom



Abschluss
Austausch Runde

Die Spielregeln

Audio & Video

Die Teilnehmenden sind stumm geschaltet, sollten die Referenten hören und die Slides sehen können.

Fragen & Inputs

Fragen können jederzeit im Q&A-Chat gestellt werden. Diese werden laufend beantwortet.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Max Klaus

stv. Leiter Operative Cybersicherheit, NCSC

NCSC

Nationales Zentrum für Cybersicherheit: Auftrag zum Schutz von kritischen Infrastrukturen in der Schweiz

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

IT-Sicherheit – eine Herausforderung für KMU

Max Klaus
stv. Leiter Operative Cybersicherheit OCS
stv. Leiter Melde- und Analysestelle Informationssicherung MELANI

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Inhalte

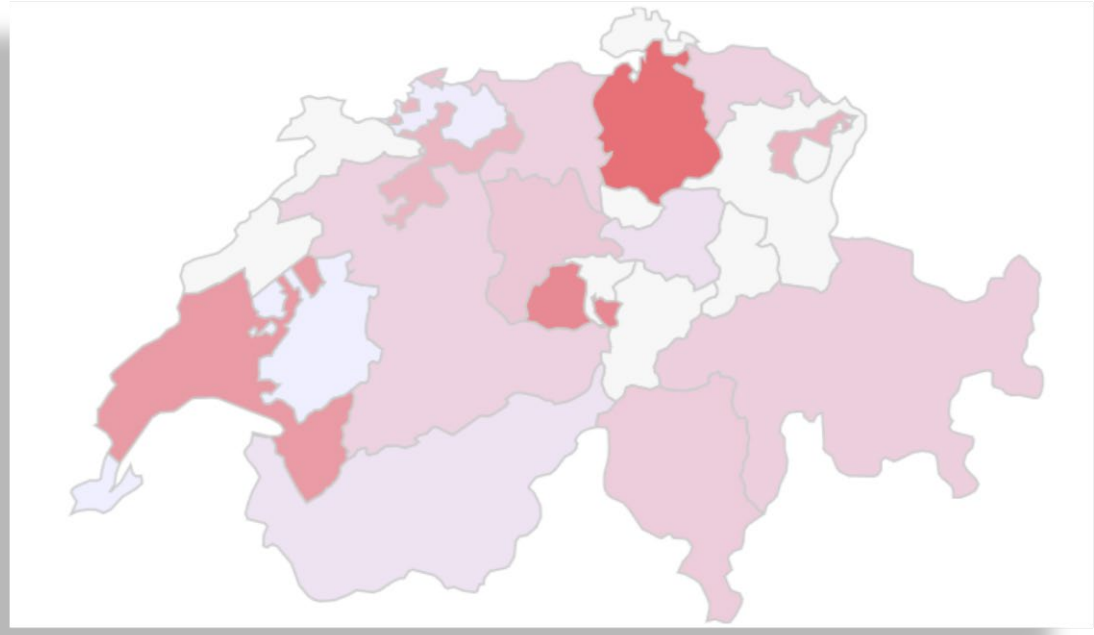
1. **Lage national / international**
2. Cyberangriffe: Ausgewählte Beispiele
3. Schlussfolgerungen/Empfehlungen

1. Lage national und international

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Lage national / international



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch »»
powered by AGVS | UPSA

Wie gefährdet sind KMU?

Wirtschaft

Neue Zürcher Zeitung

Hacker attackieren mehrere Schweizer Firmen mit Verschlüsselungs-Trojanern

In den vergangenen Wochen sind namhafte Schweizer Unternehmen Opfer von Cyberattacken geworden. Jetzt warnt die Melde- und Analysestelle Informationssicherung des Bundes (Melani) vor einer neuen Vorgehensweise der Hacker.

Gegen Cyberkriminalität kommt auch der Bund kaum an. (Symbolbild)

© Keystone

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

KMU sind gefährdeter als Grossunternehmen!

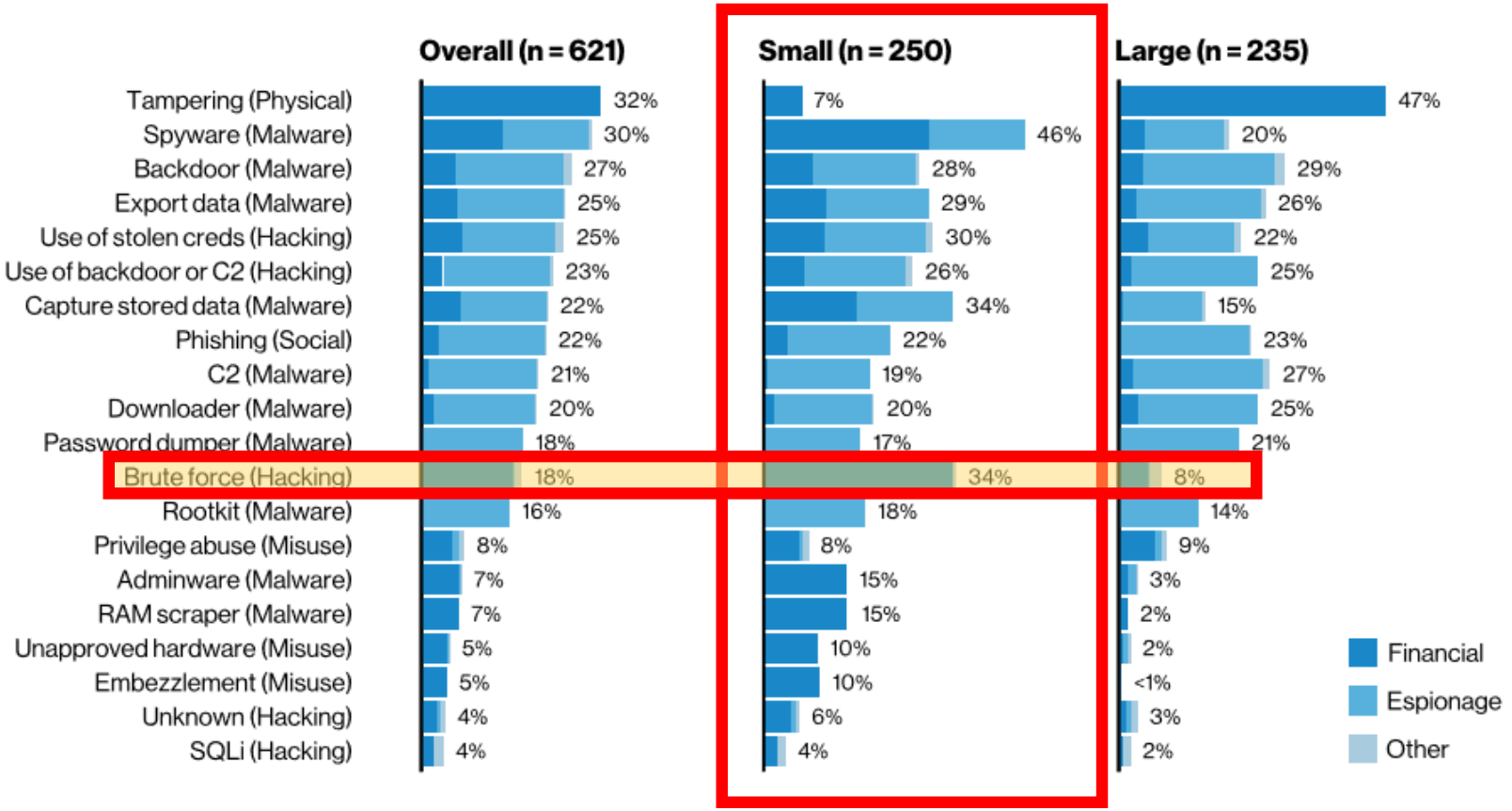


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

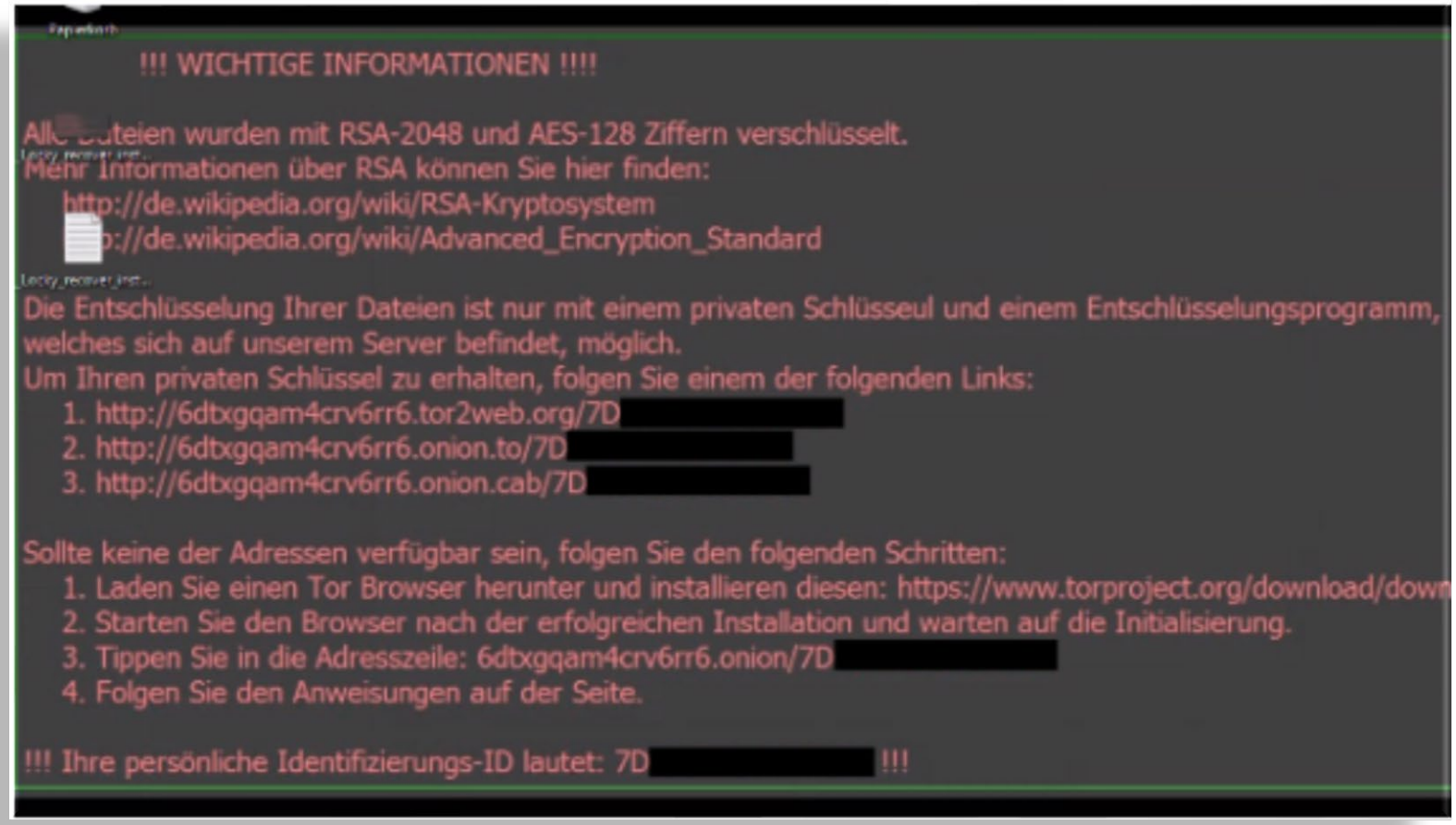
Quelle: Verizon Data Breach Report 2020 (https://enterprise.verizon.com/resources/reports/dbir/2020/smb-data-breaches-deep-dive/)

2. Cyberangriffe: Ausgewählte Beispiele

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch »»
powered by AGVS | UPSA

Verschlüsselungstrojaner



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Verschlüsselungstrojaner: Empfehlungen

- Regelmässige Datensicherung
- Datenträger nach Backup vom PC / Netz trennen
- Qualität der Backups sporadisch überprüfen
- Das Einspielen von Backups in einer ruhigen Minute üben
- Versuchen Sie, die Daten wiederherzustellen: www.nomoreransom.org
- Keinesfalls Lösegeld bezahlen!
- Information an NCSC, allenfalls Strafanzeige gegen Unbekannt bei der Kantonspolizei

AGVS | UPSA
Auto Gewerbe Verband Schweiz

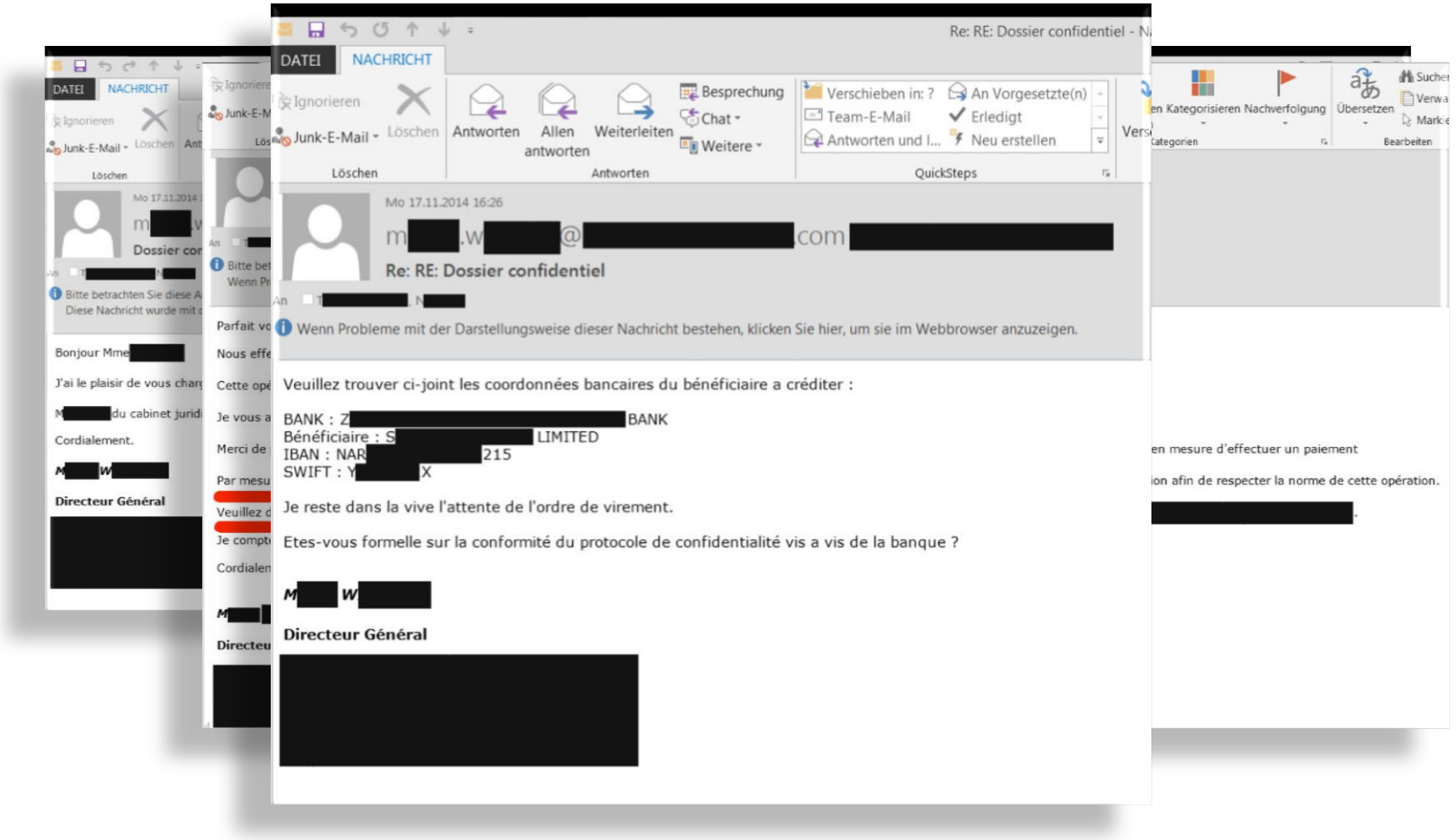
autoberufe.ch
powered by AGVS | UPSA

CEO Fraud

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

CEO Fraud



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

CEO Fraud: Empfehlungen

- Klare Weisungen bezüglich Zahlungen erteilen
- Keine internen Informationen weitergeben
- Im Zweifelsfall bei der GL nachfragen
- Ist die namentliche Erwähnung von Mitarbeitenden auf der Firmen-Website zwingend notwendig?
- Vorsicht auch bei Mails von Ihnen vermeintlich bekannten Personen
- Information an NCSC, allenfalls Strafanzeige gegen Unbekannt bei der Kantonspolizei

3. Schlussfolgerungen / Empfehlungen

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Schlussfolgerungen

- KMU sind stärker gefährdet als Grossunternehmen
- Der Mensch als schwächstes Glied in der Kette → Social Engineering
- Gesunder Menschenverstand als «Grundschutz»
- NCSC unterstützt Sie im Bedarfsfall gerne

Empfehlungen: proaktiv

Das Übliche zuerst:

- Starke Passwörter / regelmässiger PW-Wechsel
- Firewall (blacklist usw.)
- Updates
- Backups
- …

Aber:

- Technische Massnahmen allein genügen nicht!
- Organisatorische Massnahmen wie BCM, Krisenkommunikation usw. berücksichtigen!

Empfehlungen: reaktiv

Unterstützung für Unternehmen und Privatpersonen:

- Nationales Zentrum für Cybersicherheit NCSC: https://www.report.ncsc.admin.ch/de/

Strafverfolgung:

- Privatpersonen: Kantonspolizei am Wohnsitz
- Unternehmen: Kantonspolizei am Geschäftssitz

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Herzlichen Dank für Ihre Aufmerksamkeit

Wem darf ich eine Frage beantworten?

Max Klaus
Stv. Leiter operative Cybersicherheit OCS
Stv. Leiter Melde- und Analysestelle Informationssicherung MELANI

Nationales Zentrum für Cybersicherheit NCSC
Schwarztorstrasse 59
3003 Bern

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

So schützen Sie Ihre Garage

Yves Arnosti

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Was heisst Sicherheit für Sie?

Wann fühlen Sie sich sicher?

Was ist Ihr Nutzen von Sicherheit?

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

«hallo»

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

123456 **1234**

123456789

1234578 12345

111111 hallo

passwort

soleil **password**

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

1

Erkennen

- Beim Autofahren kann man ein Unfall haben (verschuldet/ unverschuldet)
- Beim Autofahren kann das Auto technisch kaputt gehen

2

Bewerten

- Unfall (verschuldet/ unverschuldet) – sehr kritisch
- Schäden – sehr kritisch

3

Vermeiden (beeinflussbar)

- Fahren nur mit 0.0 Promille
- Nur ich fahre mit dem Auto

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

4

Reduzieren

- Ein technisch gutes Auto mit Airbags, Abstandsensoren, usw.
- Jährlicher Service
- Ein Garagist des Vertrauens

5

Verlagern

- Abschluss einer Unfallversicherung
- Abschluss einer Kaskoversicherung
- TCS-Mitgliedschaft

6

Bewusst akzeptieren

- Finanzieller Schaden gemäss Wert des Autos
- Finanzieller Schaden an Leib und Leben

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

1

Erkennen

- Was schützen wir und wieso? Daten!
- Vor was schützen wir Daten?
  - Verfügbarkeit – Nutzbarkeit der Daten (Löschung)
  - Integrität – Korrektheit der Daten (Manipulation)
  - Vertraulichkeit – Nur berechtigte Personen dürfen die Daten sehen (Kopie)

2

Bewerten

- Risikomanagement (Eintrittswahrscheinlichkeit und Schadensausmass)

3

Vermeiden (beeinflussbar)

- Hauptsächlich organisatorische Massnahmen

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

4

Reduzieren

- Technische- und organisatorische Massnahmen

5

Verlagern

- Klassisch mit SLA (Service Level Agreement)
- Outsouring von Diensten
- Cyberversicherungen

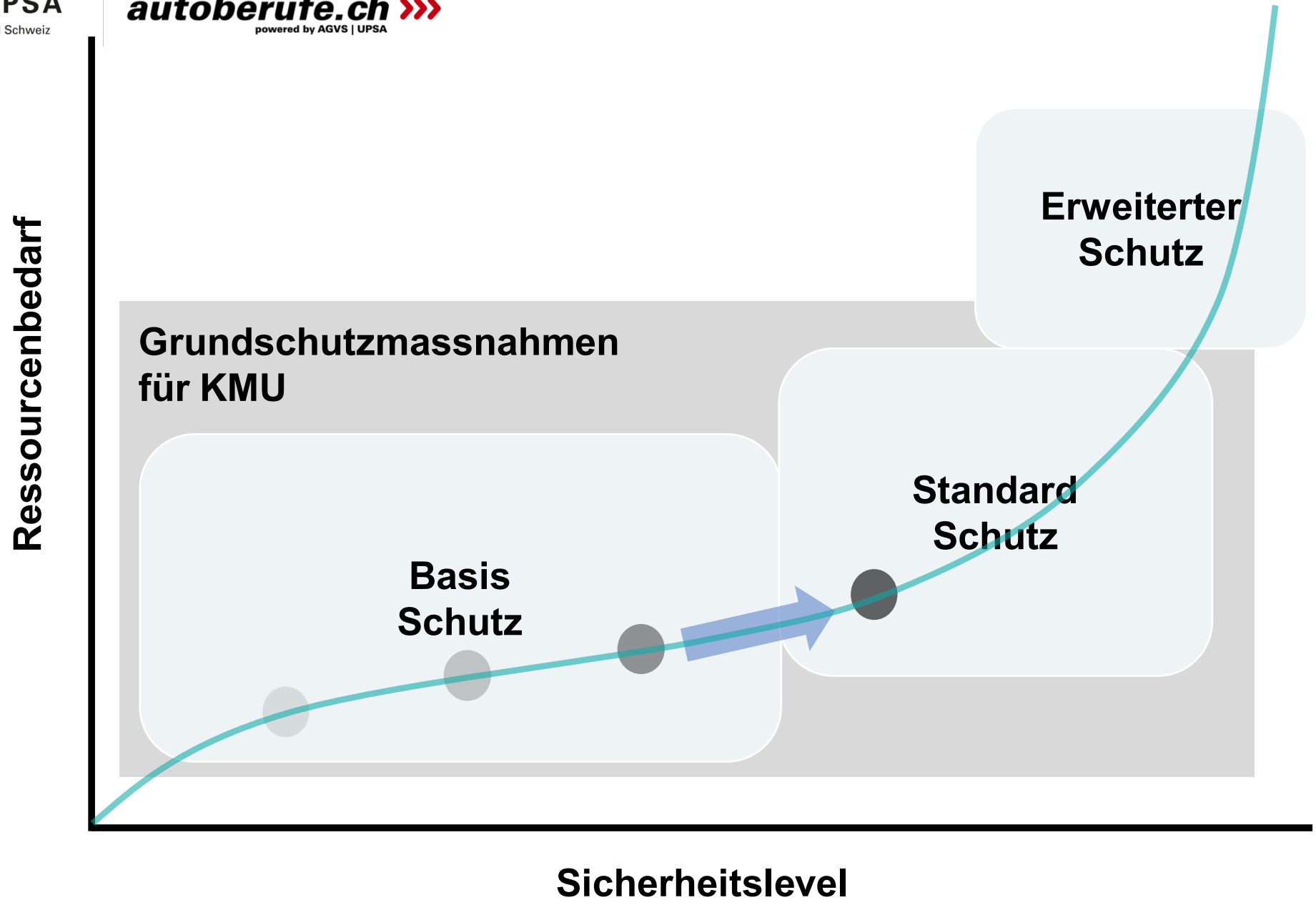
6

Bewusst akzeptieren

- Gemäss Digitalisierungsgrad des Unternehmens – Max. Datenverlust
- Gemäss der Organisation ein Katastrophenplan – Max. Wiederanlaufzeit
- Gemäss der Unternehmensstrategie – Max. Informationssicherheit
- Usw.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Work Smart

Organisatorische Massnahmen

Technische Massnahmen

Sicherheit ist keine einmalige Massnahme. IT Sicherheit **ist** ein **kontinuierlicher Prozess.**

Work Safe

Welches Passwort ist sicher?

A RichtigPferdBatterieHeftklammer

B Tr0ub4dour&3

Moderne Hackingprogramme können einzelne, bekannte Wörter (im Beispiel "Troubadour") innerhalb weniger Sekunden knacken, auch wenn Buchstaben durch Zahlen und Sonderzeichen ersetzt und zusätzliche Zeichen hinzugefügt wurden.

A RichtigPferdBatterieHeftklammer

B Tr0ub4dour&3

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Sichere Passwörter

Jedes Online-Konto verdient ein **eigenes Passwort**: Passwörter sind die Schlüssel zu unseren Daten!

Passwörter sind die **mächtigste Sicherheitsmassnahme**, welche die **User selber in der Hand** haben.

Starke Passwörter sind: **einzigartig**

- mind. **12 Zeichen** lang
- Zahlen, Gross- & Kleinbuchstaben, Sonderzeichen

Quelle: https://ibarry.ch/

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Organisatorische Massnahmen

- In einem **Rollenkonzept** definieren, welche Rechte pro Mitarbeiter notwendig sind
- **Zugriffsrechte** der Geschäftsleitung prüfen und von IT-Admin Logins trennen/einschränken
- Schulung von Mitarbeitenden und Lieferanten für den **Fernzugriff**

Technische Massnahmen

- Netzwerke mittels Firewall in Zonen aufteilen, damit wichtige Geschäftsbereiche voneinander abgeschottet sind.
- Fernzugriff mittels 2-Faktoren Authentifizierung zusätzlich absichern (z.B. SMS Code)
- Passwortregeln für Mitarbeitende
- Definierte Rollen mit den Zugriffsrechten koppeln und einschränken

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Mitarbeitende als das grösste Sicherheitsrisiko

> 80 %

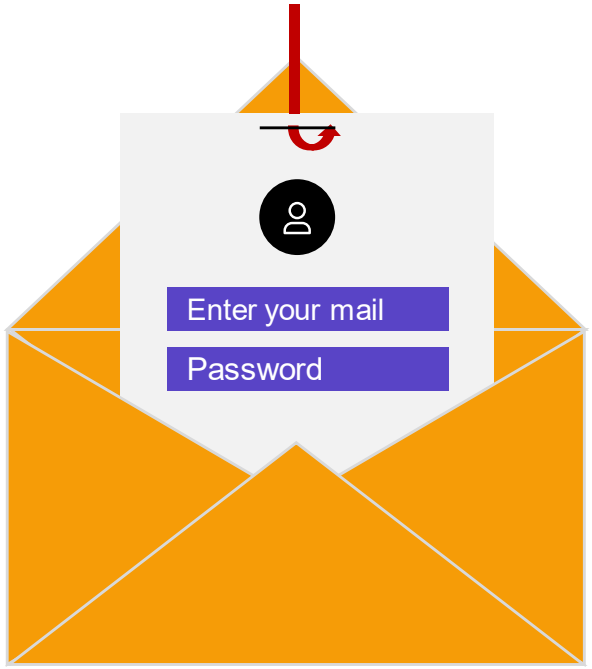
aller Cyberangriffe auf Fehler von Mitarbeitenden zurückzuführen.

- **Sicherheitsrichtlinien**
- **Benutzerrechte** einschränken
- Mitarbeitende **sensibilisieren, Umgang mit E-Mails**

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Erkennung von Phishing Mails



- Kryptische Absender-Mail-Adresse
- Angaben persönlicher Daten
- Verdächtige Anhänge
- Aufforderung, sofort zu handeln
- Link-Text & Link stimmen nicht überein
- Schreibfehler & einfache Sprache

AGVS | UPSA
Auto Gewerbe Verband Schweiz

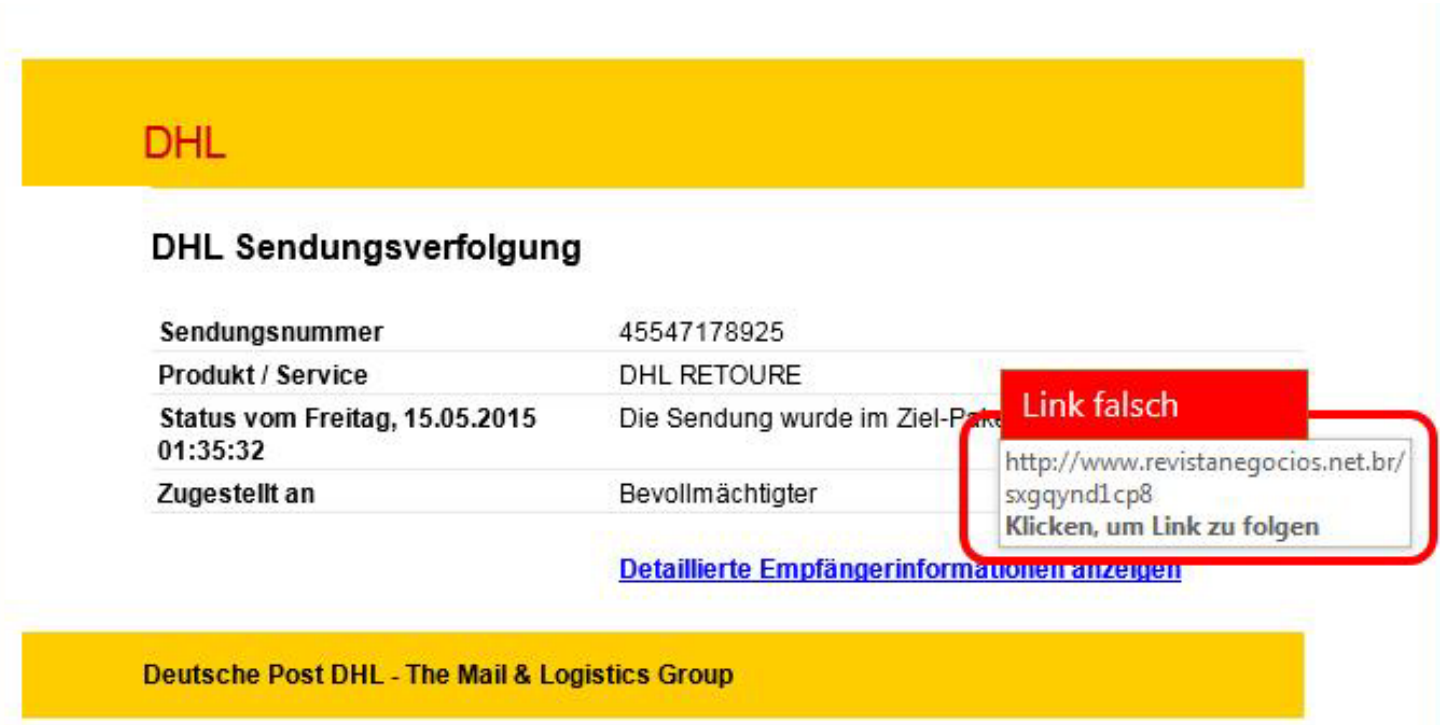
autoberufe.ch
powered by AGVS | UPSA

⚠ **Gefälschte Absenderadressen**

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

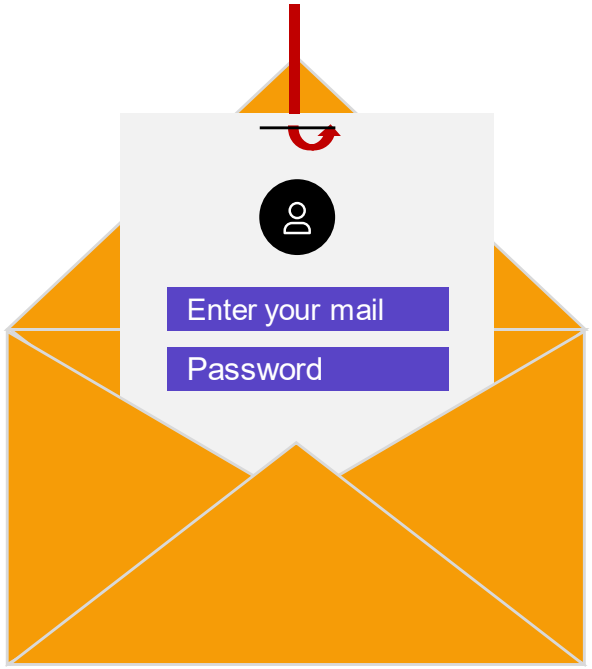
⚠ Vorgeblich vertrauenswürdiger Link



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Phishing Mails: Tipps & Tricks



- Geben Sie **nie Benutzername, Passwort, Kreditkarten-** oder **detaillierte Adressangaben** via E-Mail weiter.
- Seien Sie misstrauisch gegenüber E-Mails mit **Rechtschreib- & Grammatikfehlern**.
- Öffnen Sie nur **E-Mail-Anhänge** von Absendern, denen Sie **vertrauen** und die Sie **erwartet** haben.
- "Klick hier" – **Link** in einer E-Mail? Fahren Sie mit der Maus darüber und prüfen Sie ihn auf Auffälligkeiten.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Organisatorische Massnahmen

- Sensibilisierung und Schulung von Mitarbeitenden im Umgang mit Emails, Webseiten, Passwörtern etc.
- IT-Security als Teil des Einarbeitungsplans für neue Mitarbeitende
- Anlaufstellen für Fragen von Mitarbeitenden

Technische Massnahmen

- Schutz des Netzwerks durch eine Firewall
- Umfassender, flächendeckender Malwareschutz von Endgeräten, Servern, Cloud- und E-Mail Services
- Makroausführung einschränken; Internet- und Spamfilter installieren

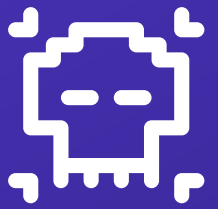
AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Netzwerksicherheit durch Segmentierung

- Kritische Daten, Prozesse und Systeme in getrennten Netzwerken
- Gästenetzwerk trennen
- Nutzergruppen erstellen

Anzahl neue Schadsoftware-Programme pro Tag?



350'000

Welches Betriebssystem setzen Sie ein?

A Windows 7

B Windows 8

C Windows 10

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Sicherheitslücken durch fehlende Updates

- Betriebssysteme, Programme & Anwendungen **aktuell halten**
- **Patch- & Update-Management** für Hardware & Anwendungen

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Organisatorische Massnahmen

- Eine Person definieren, die für die Verwaltung und periodische Überprüfung der Updates verantwortlich ist
- Gemäss Risikobeurteilung veraltete Systeme ablösen und bestehende physisch schützen
- Regelmässig über Trends und neue Technologien informieren

Technische Massnahmen

- Automatisiertes Updatemanagement
- Nur aktuelle Betriebssysteme und Applikationen einsetzen
- Alte Systeme vom Netzwerk isolieren

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Ein funktionierendes (!) Backup kann Ihren Tag retten. ;-)

- Backups vom System trennen
- Je regelmässiger, desto besser

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Organisatorische Massnahmen

- Eine Person für die Umsetzung und Überprüfung definieren
- Externe Speicherung des Backups sicherstellen
- Notfall-Organisation bestimmen, Prozesse definieren und alle Mitarbeiter informieren
- Rollen und Abläufe regelmässig überprüfen und Datenrückführung testen

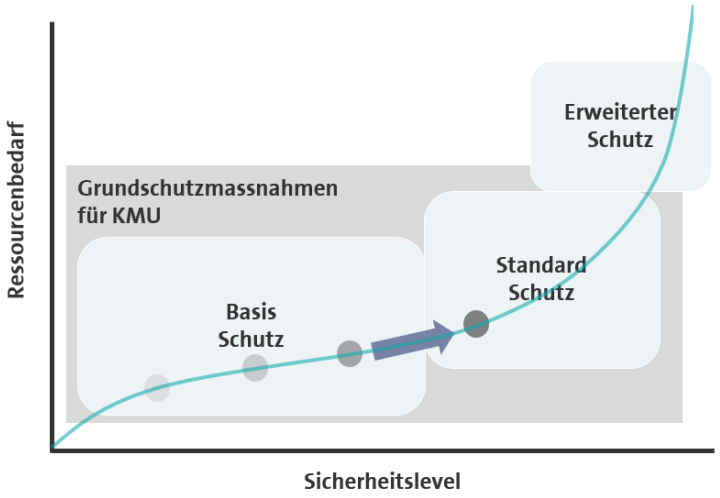
Technische Massnahmen

- Automatisierter, schreibgeschützter Backup-Prozess inkl. Verschlüsselung
- Wenn obiges nicht möglich: Backup-Medium vom Netzwerk trennen und offline lagern

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Security Checkliste

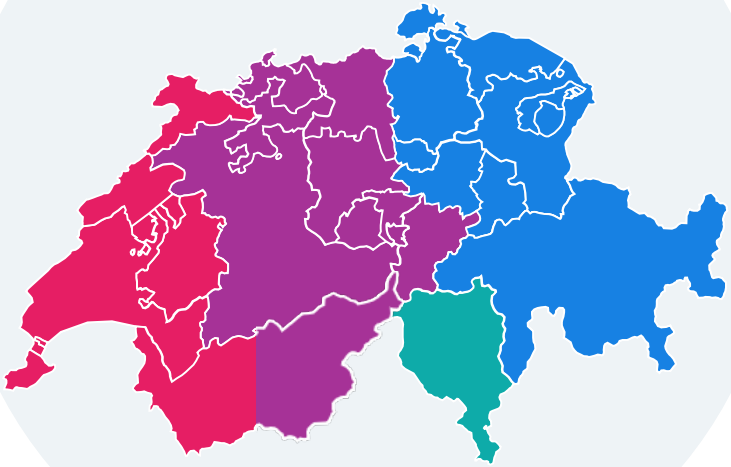


- Antivirus & Firewall
- Netzwerksicherheit
- Betriebssysteme
- Datensicherung
- Backups
- Mitarbeitende
- Passwörter
- Mobile

Unsere IT-Lösung für Ihre Garage!
Alles aus einer Hand. Wir finden Ihren persönlichen Partner.
www.swisscom.ch/garage

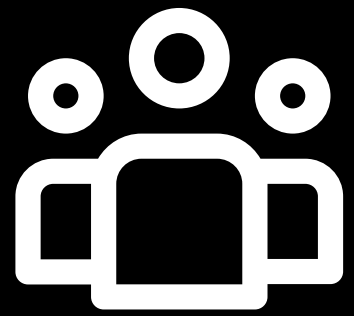
AGVS | UPSA X

Schweizweit starkes Swisscom Partnernetz



AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA



F&A

Austauschrunde

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

F

Verschlüsselungstrojaner. Was ist wenn die Datensicherung auch verschlüsselt wurde? Wie kann ich das umgehen?

A

Das Backup sollte zwingend getrennt aufbewahrt werden, so dass ein Verschlüsselungstrojaner dieses nicht auch verschlüsseln kann.

F

Sind Sicherungen auf ein NAS demselben Risiko ausgesetzt wie eine externe Festplatte?

A

Ja, sofern das NAS immer läuft und somit erreichbar ist.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

F

Sind Sicherungen über Ethernet in ein anderes Subnetz mit ssh und rsync auf ein anderes NAS eine sichere Variante um die Daten für den Verschlüsselungstrojaner unerreichbar zu machen?

A

Sofern zwischen den verschiedenen Subnetzen zusätzliche Sicherheitsvorkehrungen (z.B. Firewall) aktiv sind, kann dies das Risiko allenfalls reduzieren. Müssen aber die Backup-Dateien irgendwie auf dieses NAS gelangen, kann auch der Verschlüsselungstrojaner diesen Weg gehen.

F

Was halten sie von Passwortmanager und wenn ja welcher?

A

Pro Login sollte ein Passwort grundsätzlich immer nur 1x genutzt werden. Zudem sollten die Passwörter möglichst lang und komplex sein. Dadurch wird es immer schwieriger sich die Passwörter zu merken, auf ein Post-it auf dem Pult sollte verzichtet werden. Um sich nun die Passwörter zu merken, eignet sich definitiv ein Passwortmanager. WICHTIG: jeder Passwortmanager hat ein sogenanntes Master-Login mit welchem man dann auf alle seine Passwörter zugreifen kann. Dieses Passwort muss zwingend lang und komplex sein und darf nicht weitergegeben werden.

F

Antivierungsprogramme: Wir hatten Vieren trotz diesen teuren Programme. Sind diese überhaupt wirksam oder hinken diese nicht hinten nach?

A

Einen 100%igen Schutz gibt es leider nie. Ein Antivirenprogramm ist ein wichtiger Bestandteil eines Sicherheitskonzeptes. Auf der einen Seite arbeiten AV-Programme mit der Erkennung von bekannten Viren. Die weitaus schwierigere Aufgabe ist es, neue, noch unbekannte Viren zu erkennen. Hier versuchen die unterschiedlichen Herstellern dies auf unterschiedliche Arten. Wichtig, damit ein Antivirenprogramm zuverlässig schützen kann, muss zwingend sämtliche eingesetzte Software (inkl. Betriebssystem) immer aktuell sein, somit sämtliche Updates sollten zeitnah installiert werden.

F

Sind die Verschlüsselungstrojaner ausschliesslich auf Windos als Einfallstor beschränkt oder mittlerweile auch auch Unixartige Betriebssysteme ausgerichtet?

A

Sämtliche Betriebssysteme sind davon betroffen.

F

Gibt es auch Angriffe von der die Hardware schaden nimmt?

A

Ja, in gewissen Fällen kann auch gezielt versucht werden, einen Hardware Schaden herbeizuführen. Grundsätzlich verfolgen die Angreifer aber finanziellen Ziele, und um diese zu erreichen wird nicht prinzipiell versucht einen Hardware Schaden zu verursachen.

F

Wie verhält sich der Teamviewer mit Fernzugriff auf Angriffe? Ist das auch sicher (Homeoffice)?

A

Die Verbindungen mit Teamviewer sind grundsätzlich verschlüsselt und gelten nicht grundsätzlich als Einfallstor für einen Angriff. Wichtig ist, wie der Teamviewer betrieben wird, so dass nicht mit dem Standardpasswort gearbeitet wird resp. auf den Computer zugegriffen werden kann. Wird mit einem Teamviewer Account gearbeitet, ist es zwingend die 2 Faktor-Authentifizierung zu aktivieren.

F

Was mache ich wenn ich ein fragwürdiges mail erhalte? Löschen wäre das einfachste. Meist bin ich mir aber dann noch nicht sicher ob es trotzdem wichtig ist. Was empfehlen Sie?

A

Im Zweifel, aufgrund des Absenders und / oder des Betreffs, versuchen den potenziellen Absender z.B. telefonisch kurz zu kontaktieren.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

F

Was ist eine übliche Risikobewertung für Public Clouds? Früher wurde meist davon abgeraten, da (sensible) Daten dort im Ausland gespeichert werden und die eigene Angriffsoberfläche um die Vulnerabilities des Cloudanbieters und der aller Teilnehmer erweitert wird. Hat sich dies heute verändert?

A

Inzwischen bieten verschiedene Public Cloud Anbieter auch eine Datenhaltung in Schweizer Rechenzentren an. Gewisse Anbieter zertifizieren gewisse Dienste auch für sensible Daten. Sobald die Infrastruktur mit dem Internet verbunden ist, kann bei einer lokalen Infrastruktur nicht von einem geringeren Risiken im Vergleich zu Cloud Services gesprochen werden.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

F

Nachdem ein Mitarbeiter einen verdächtigen Anhang geöffnet hat. Kann man dann noch etwas Sinnvolles unternehmen oder ist dann bereits alles zu spät?

A

Den betroffenen Computer sofort ausschalten, allenfalls die gesamte Infrastruktur und den eigenen IT Partner umgehend kontaktieren.

F

Wenn ich mein Backup Sicherung austausche und schon angegriffen wurde wird die neue Sicherung die ich anschliesse auch verschlüsselt?

A

Meistens ist der Verschlüsselungstrojaner immer aktiv und sucht nach neuen, unverschlüsselten Medien. Wird ein entsprechendes gefunden, wird versucht, auch dieses zu verschlüsseln.

AGVS | UPSA
Auto Gewerbe Verband Schweiz

autoberufe.ch
powered by AGVS | UPSA

Bringen Sie Ihre IT in Sicherheit!