handelskammer beider basel

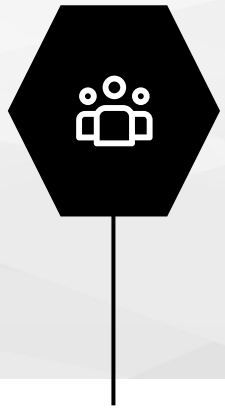
Herzlich Willkommen

IT Sicherheit ⋆ ⋆ ⋆
eine Herausforderung für KMU

handelskammer beider basel

Cyberbedrohung
Max Klaus,
stv. Leiter Operative
Cybersicherheit, NCSC

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



Abschluss
Austausch Runde

IT-Sicherheit – eine Herausforderung für KMU

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

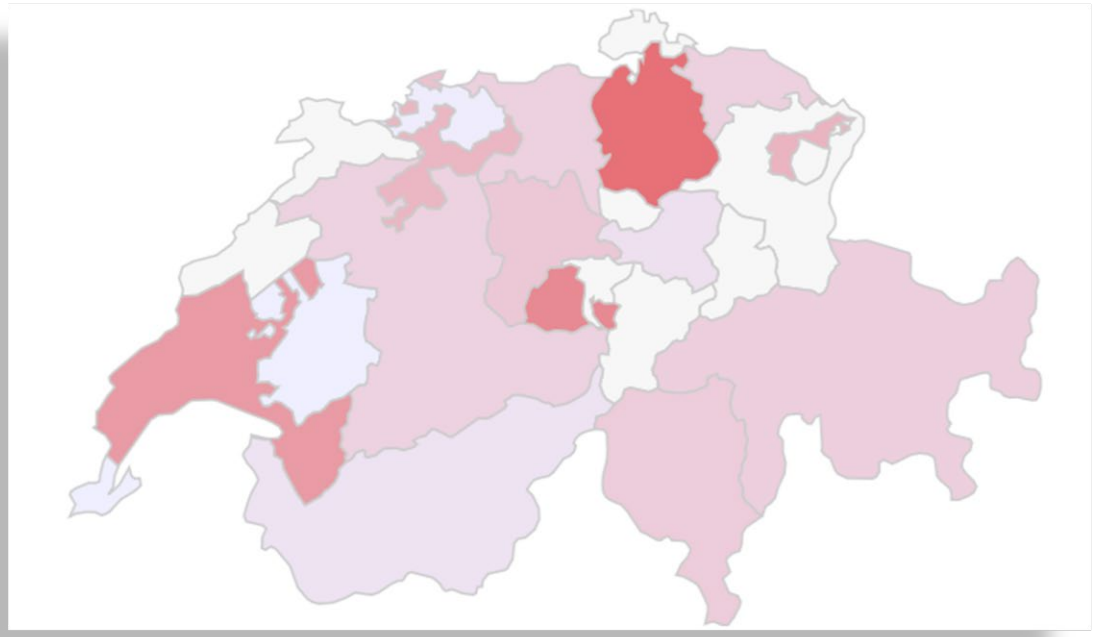
Generalsekretariat EFD
Nationales Zentrum für Cybersicherheit NCSC

Inhalte

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

1. Lage national und international

Lage national / international



Wie gefährdet sind KMU?

SRF News Sport Meteo Kultur DOK

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

KMU sind gefährdeter als Grossunternehmen!

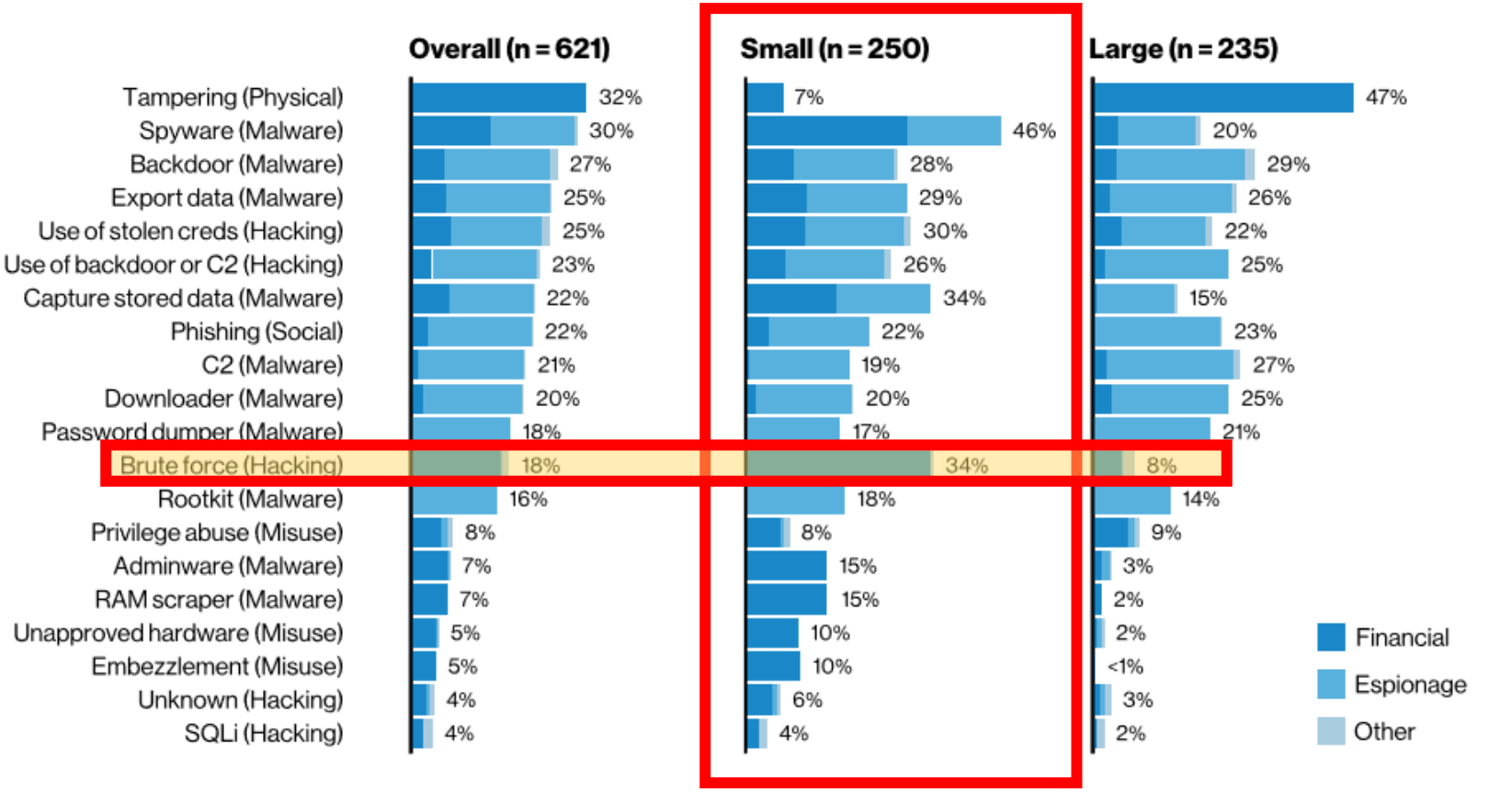
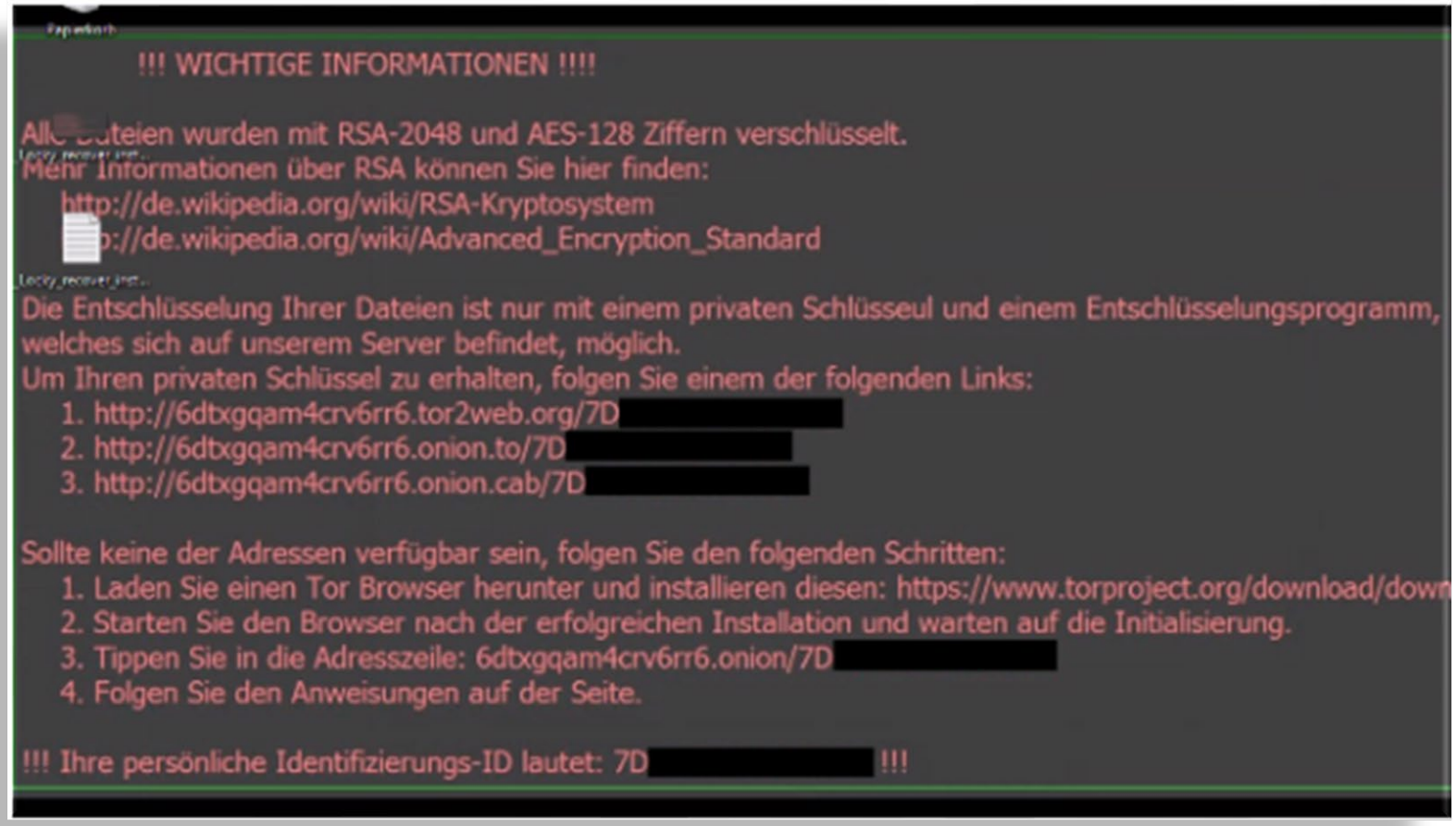


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

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

2. Cyberangriffe: Ausgewählte Beispiele

Verschlüsselungstrojaner

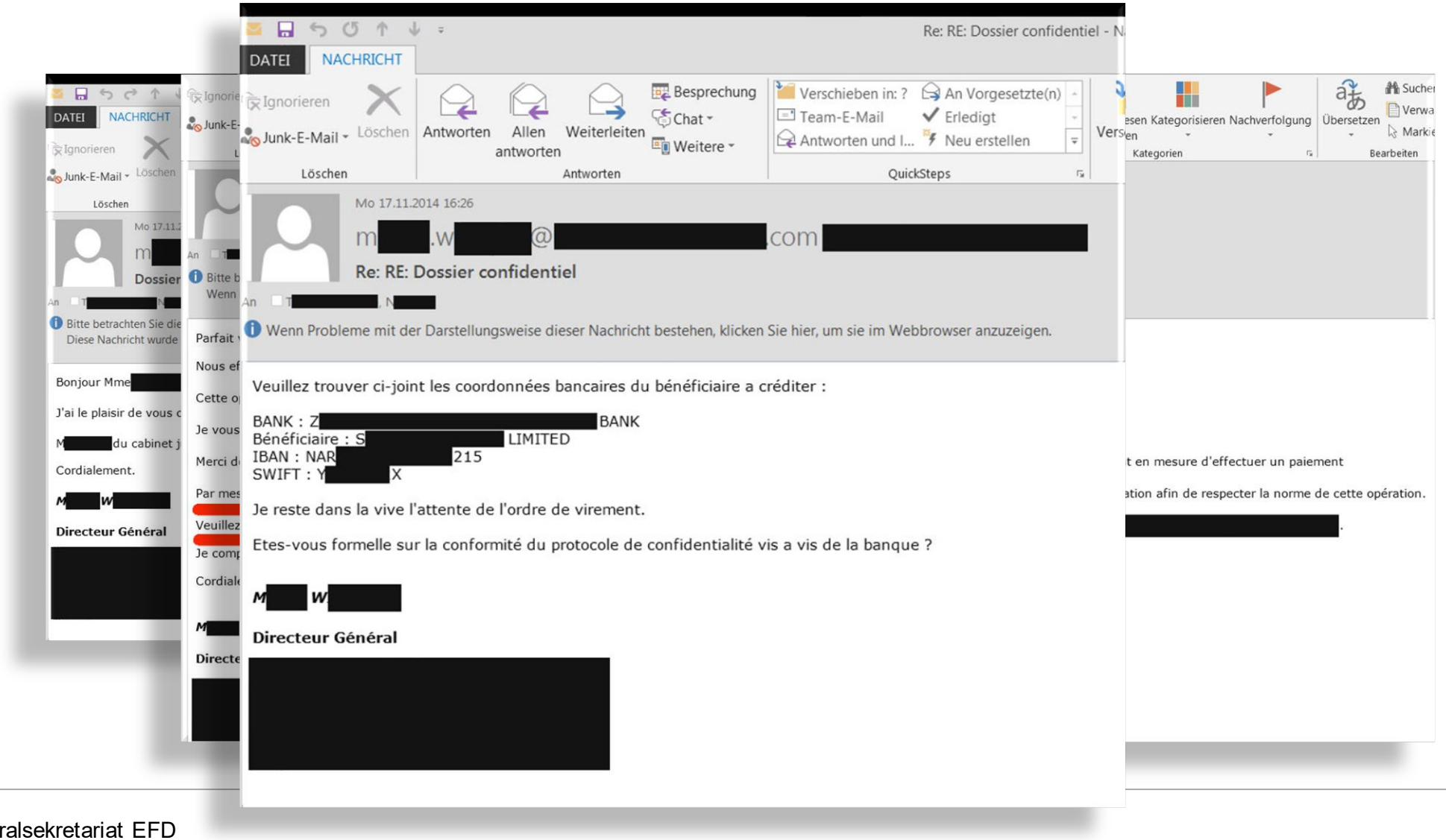


Verschlüsselungstrojaner: Empfehlungen

- 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

CEO Fraud

CEO Fraud


DATEI
NACHRICHT
Re: RE: Dossier confidentiel - N
Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Verschieben in: ?
Team-E-Mail
Antworten und l...
An Vorgesetzte(n)
Erledigt
Neu erstellen
Löschen
Antworten
QuickSteps
Kategorisieren
Nachverfolgung
Übersetzen
Kategorien
Bearbeiten
Mo 17.11.2014 16:26
Re: RE: Dossier confidentiel
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Veuillez trouver ci-joint les coordonnées bancaires du bénéficiaire a créditer :
BANK : Z BANK
Bénéficiaire : S LIMITED
IBAN : NAR 215
SWIFT : Y X
Je reste dans la vive l'attente de l'ordre de virement.
Etes-vous formelle sur la conformité du protocole de confidentialité vis a vis de la banque ?
Directeur Général

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

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

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

So schützen Sie Ihr KMU

Yves Arnosti

swisscom

« hallo »

swisscom

123456 **1234**

123456789

1234578 12345

111111 hallo

passwort

soleil **password**

swisscom

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.

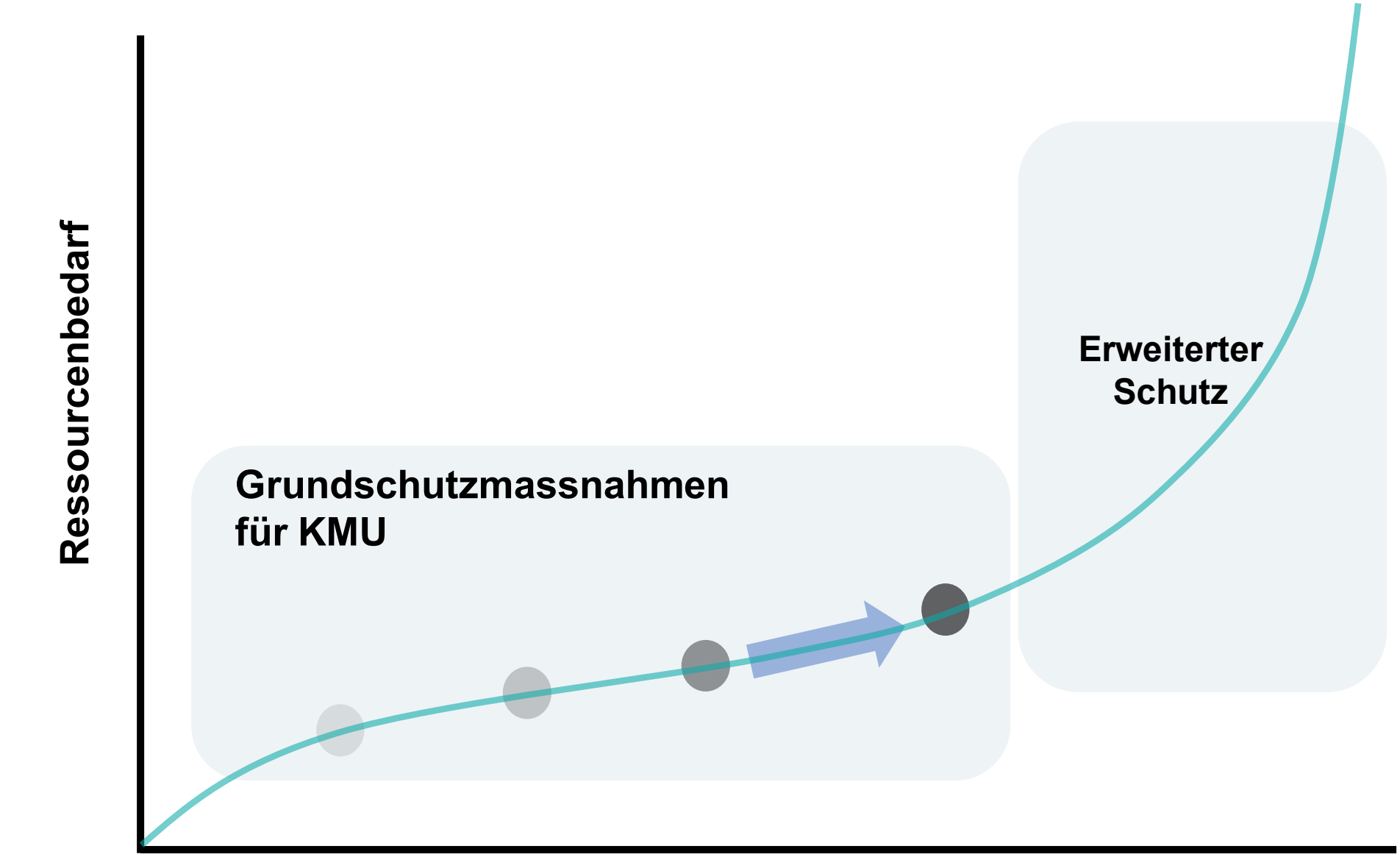
A RichtigPferdBatterieHeftklammer

B Tr0ub4dour&3

Was heisst Sicherheit für Sie?

Wann fühlen Sie sich sicher?

swisscom


Ressourcenbedarf
Grundschutzmassnahmen
für KMU
Erweiterter
Schutz
Restrisiko hoch
Sicherheitslevel
Restrisiko klein

swisscom

Organisatorische Massnahmen

Technische Massnahmen

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

Work Smart

Work Safe

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/

swisscom

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

swisscom

Mitarbeitende als das grösste Sicherheitsrisiko

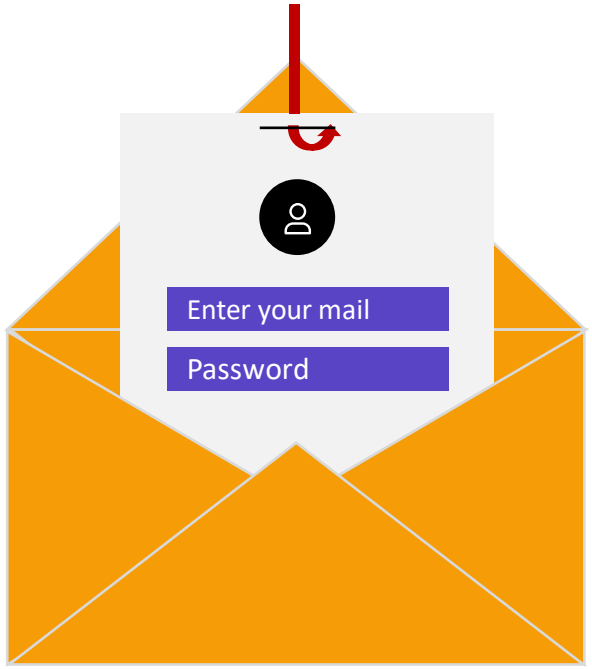
> 90 %

aller Cyberangriffe auf Fehler von Mitarbeitenden zurückzuführen.

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

swisscom

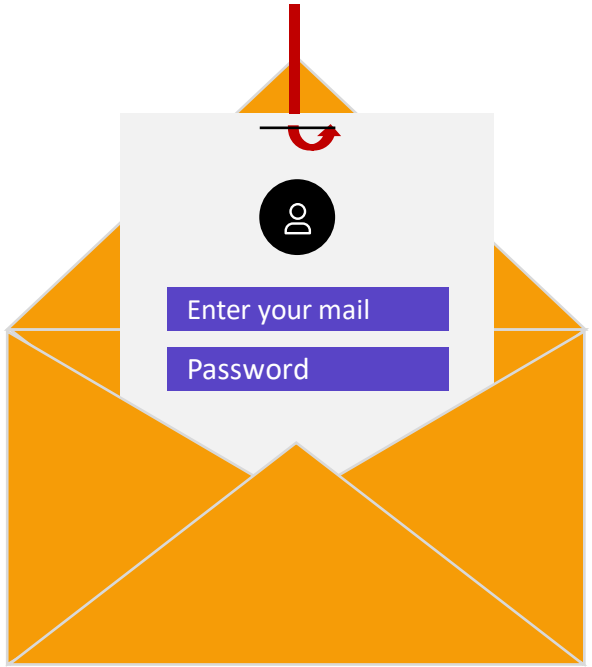
Erkennung von Phishing Mails



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

swisscom

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.

swisscom

Security-Schulung für Ihre Mitarbeitenden

Geben Sie dem Hacker keine Chance

In diesem kurzen Lernspiel von 15 Minuten zeigen wir Ihnen in drei Level, wie Sie sich bereits dank einfachen Verhaltensregeln und Tipps besser schützen können.

www.swisscom.ch/security-schulung

swisscom

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

swisscom

Netzwerksicherheit durch Segmentierung

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

swisscom

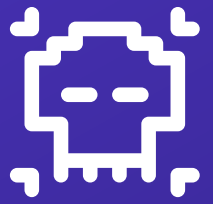
Welches Betriebssystem setzen Sie ein?

A Windows 7

B Windows 8

C Windows 10

Anzahl neue Schadsoftware-Programme pro Tag?



350'000

Sicherheitslücken durch fehlende Updates

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

swisscom

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

swisscom

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

- Backups vom System trennen.
- Je regelmässiger, desto besser.

swisscom

Organisatorische Massnahmen

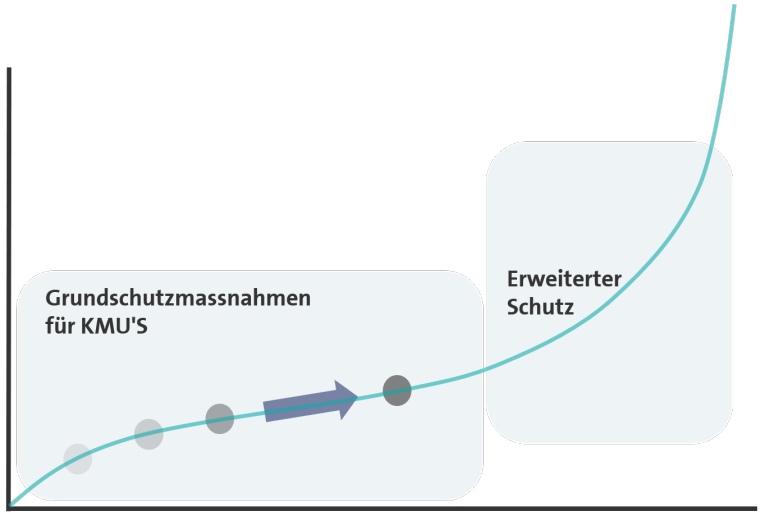
- Eine Person für die Umsetzung und Überprüfung definieren
- Externe Speicherung des Backups sicherstellen
- Notfall-Organisation bestimmen, Prozesse definieren und alle Mitarbeiter informieren
- Rollen und Abläufe regelmässig überprüfen und Datenrückführung testen

Technische Massnahmen

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

swisscom

Security Checkliste



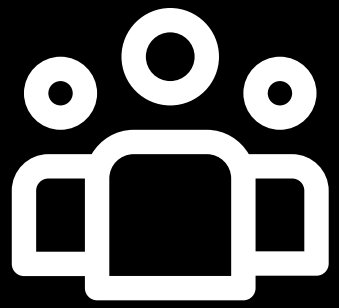
- Antivirus & Firewall
- Netzwerksicherheit
- Betriebssysteme
- Datenschutz
- Backups
- Mitarbeitende
- Passwörter
- Mobile

swisscom

Unsere IT-Lösung für Ihr KMU!
Alles aus einer Hand. Wir finden Ihren persönlichen Partner.

handelskammer beider basel x

handelskammer beider basel



Abschluss

Austausch Runde

Bringen Sie Ihre IT in Sicherheit!