InfoGuard
SWISS CYBER SECURITY

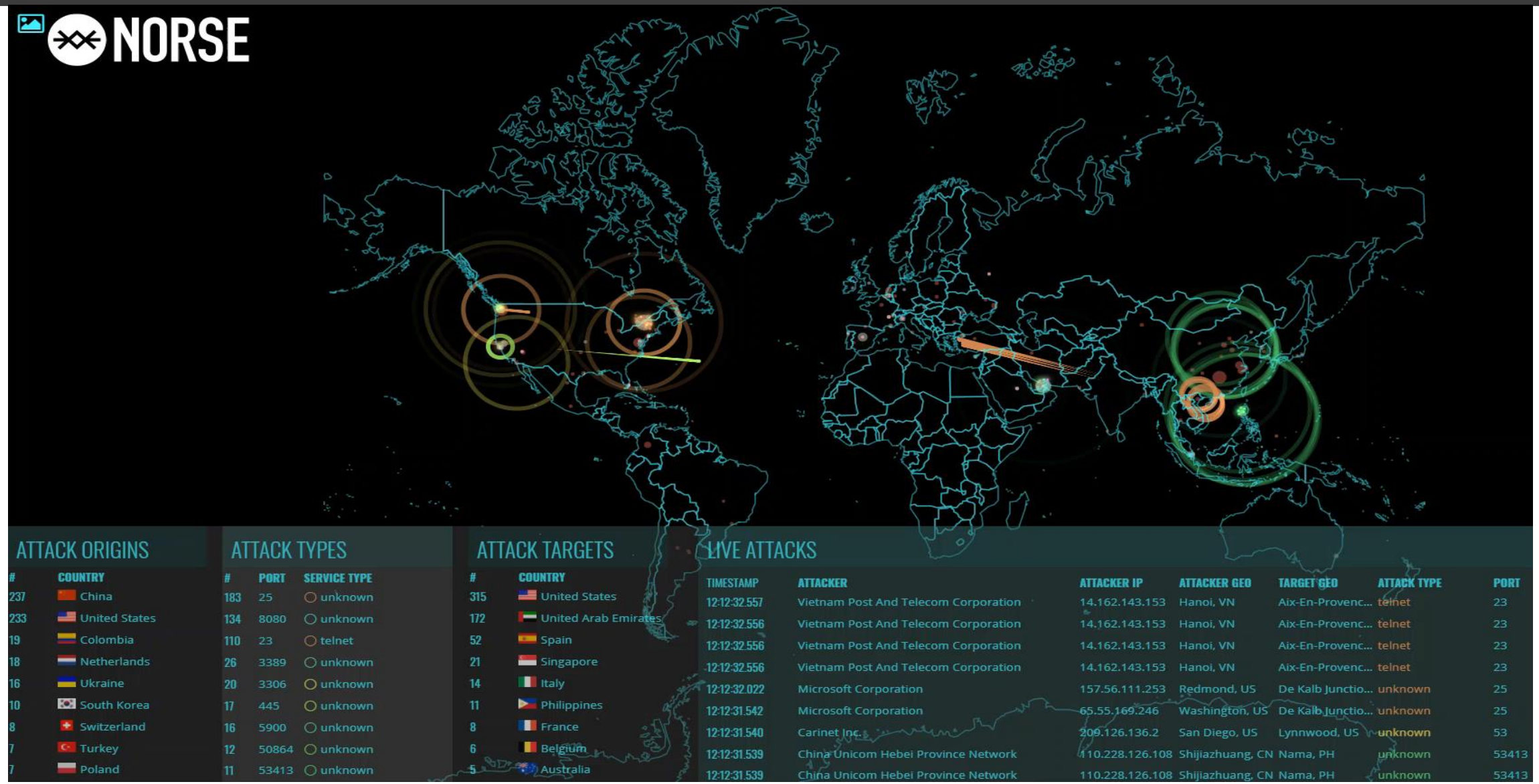
CYBER SECURITY – WIE HACKER AN VERTRAULICHE INFORMATIONEN KOMMEN

26. November 2018

«Cyber Security ist vielschichtig. Ein zuverlässiger Schutz Ihrer Werte – Informationen, Mitarbeiter, Prozesse und Infrastruktur – lässt sich nur über einen strukturierten, methodischen Sicherheitsprozess erreichen.»

Franco Cerminara
Chief Consulting Officer, InfoGuard AG
Tel. +41 41 749 19 62
Mob. +41 79 308 83 16
franco.cerminara@infoguard.ch

Steigende Cyberkriminalität

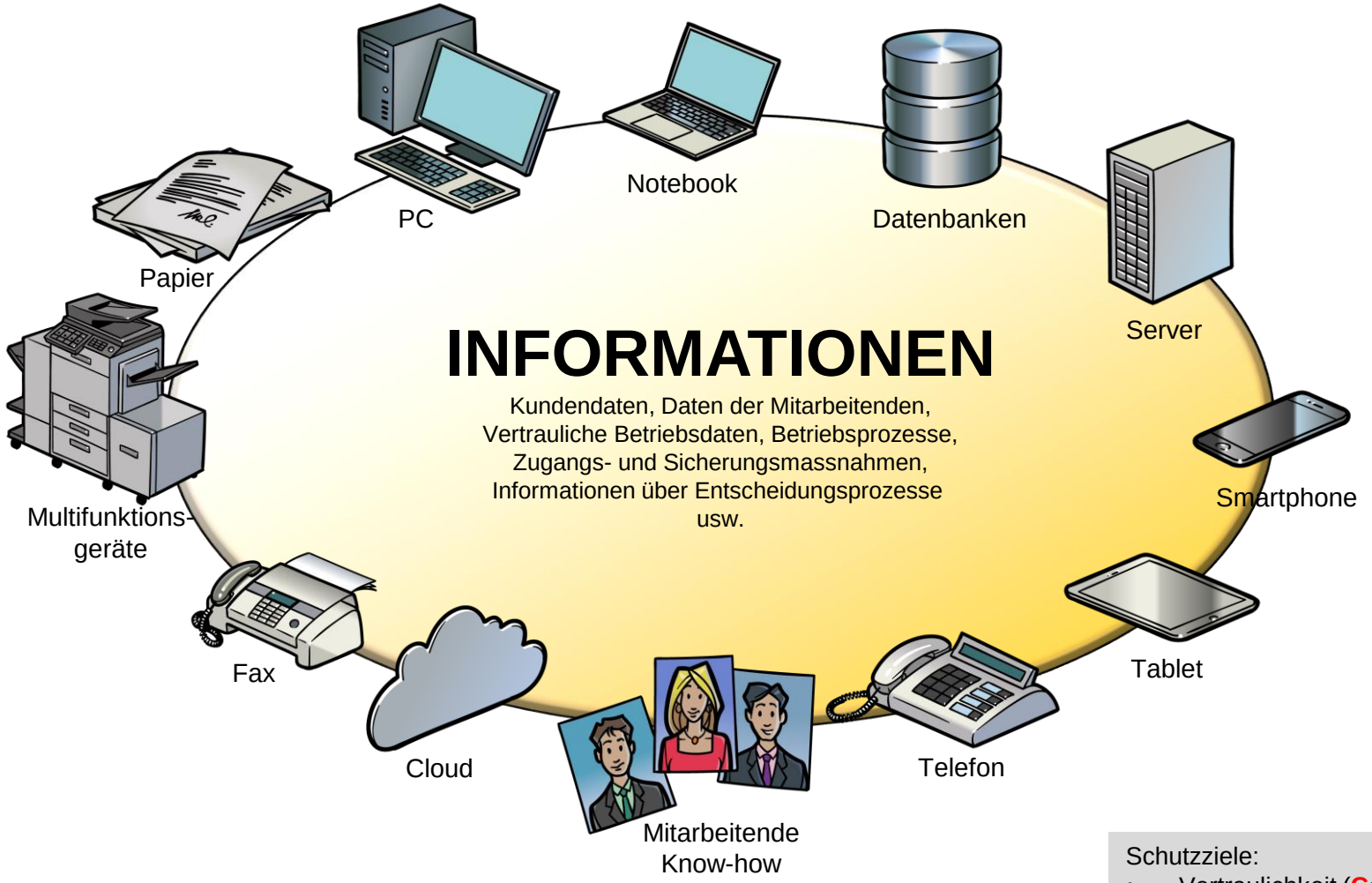


Cyberkriminalität - einige Fakten

Quelle: KPMG 2017 «Clarity on Cyber Security»

- Cyber Crime ist ein **grosses Geschäft**: Mehr gezielte Angriffe
- **Angreifer** sind professionell, geduldig, beharrlich, hochentwickelt, gut organisiert und gut finanziert.
- **Verschwindender Perimeter**: Cloud Services, Mobile Geräte, IoT, Digitalisierung etc.
- Stetig **neue Sicherheitslücken** und verdeckte Angriffe
- Angriffe nicht nur auf Technologie, sondern vermehrt auf **Menschen** und **Prozesse**
- Ein **ungleicher Kampf**: Angreifer muss 1x Erfolg haben – Verteidiger immer.

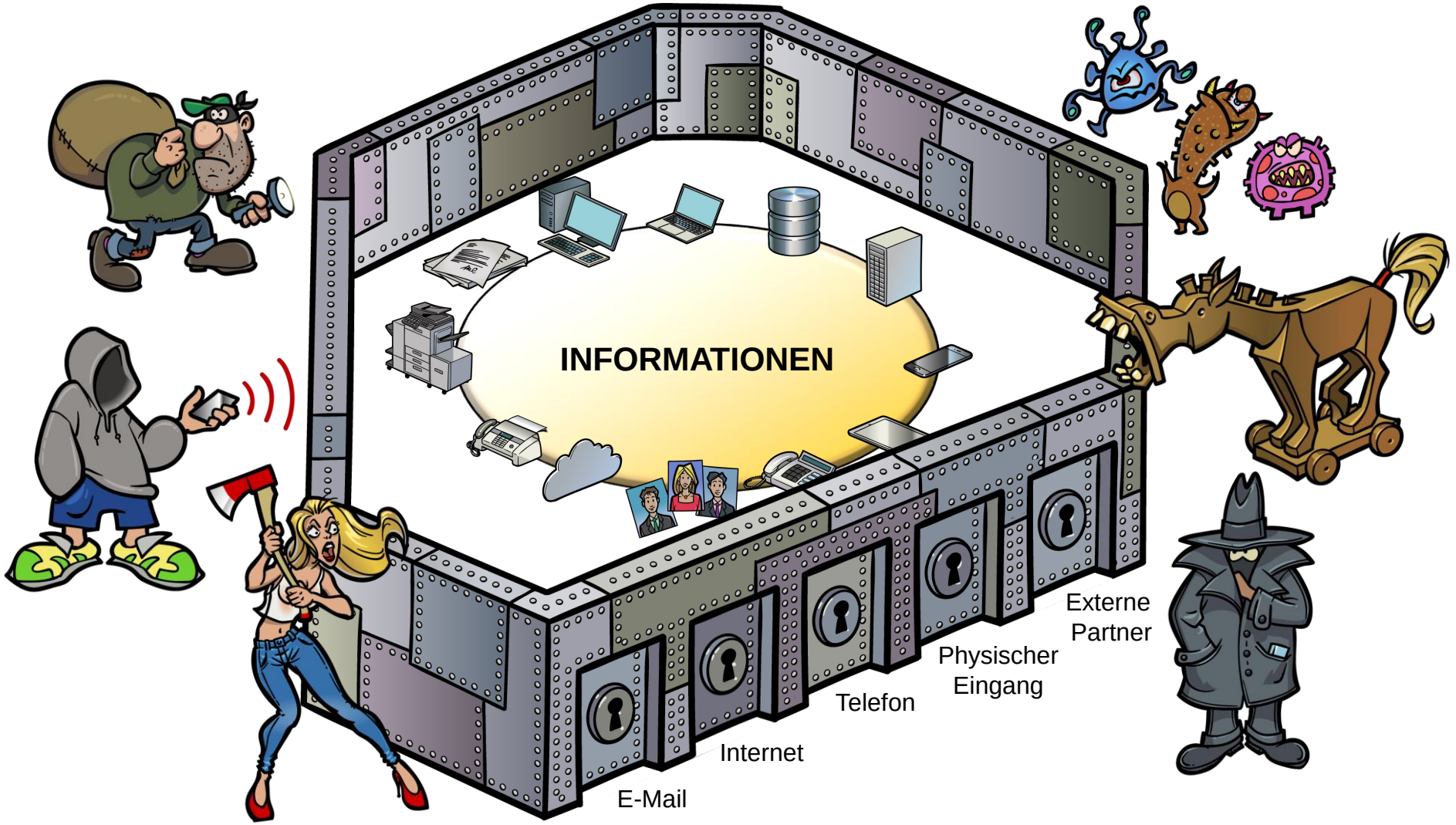
Informationen



Schutzziele:

- Vertraulichkeit (**C**onfidentiality)
- Integrität (**I**ntegrity)
- Verfügbarkeit (**A**vailability)

Bedrohungen



Fakten zu E-Mail: InfoGuard mit 100+ Mitarbeiter

InfoGuard
SWISS CYBER SECURITY

945’204
Received Mails

795'392
Rejected Mails / Bad Reputation

60'268
Rejected Mails / Spam

89'544
CLEAN: 9.5% of all Mails received

Der grösste Risikofaktor?

... der Mensch!

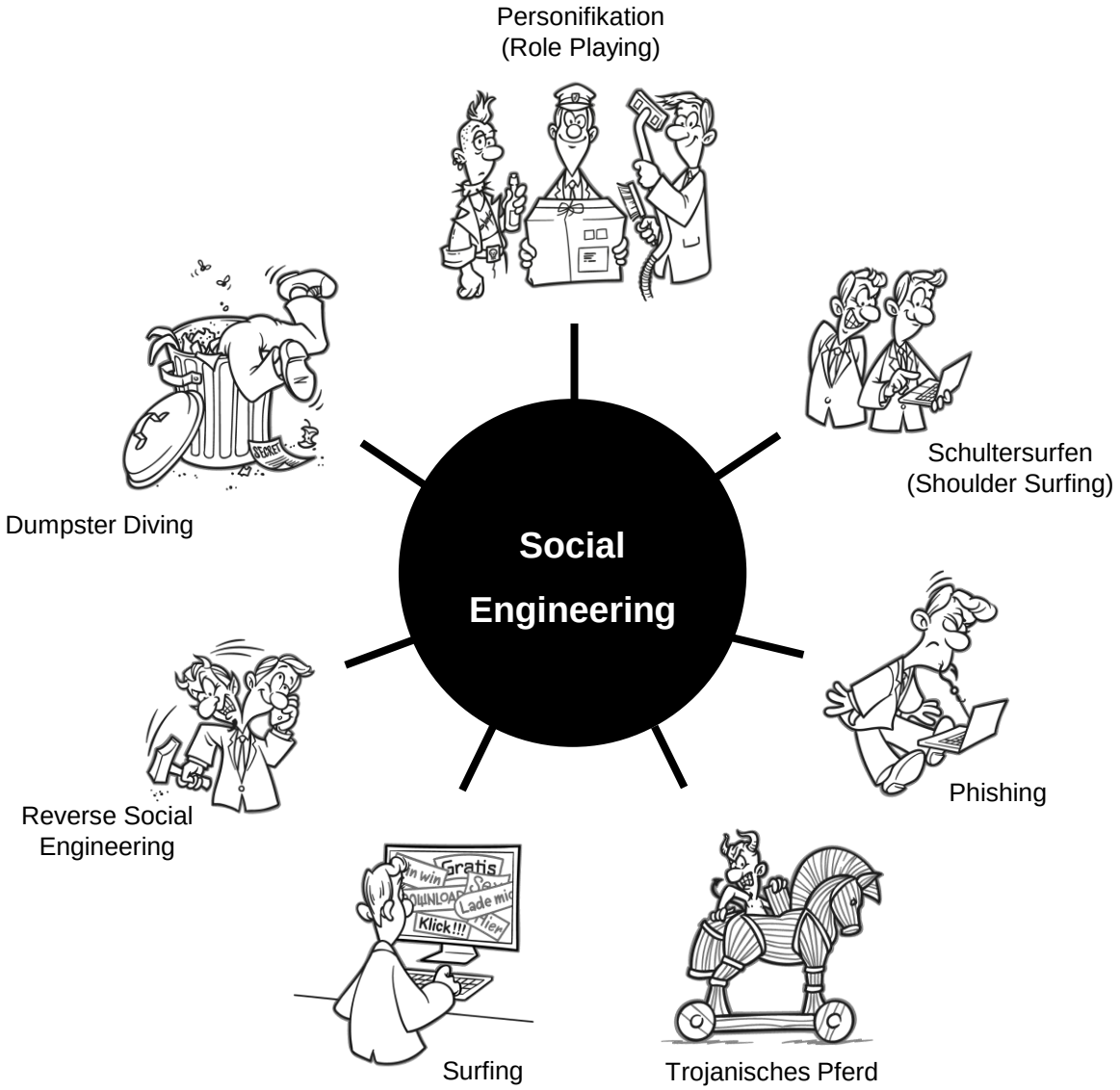
Was ist Ihr Passwort?

Was ist «Social Engineering»?

Das Social Engineering ist eine **Spionageattacke**, die sich auf **sozialer** Ebene abspielt. Ein Social Engineer versucht sein Opfer so zu **manipulieren**, auch mit **psychologischen** Tricks, dass es ihm die **sensitiven Informationen** gibt, die er haben möchte.

«Amateurs tend to attack machines, whereas professionals target people.»
Bruce Schneier

Ausprägungen des «Social Engineering»

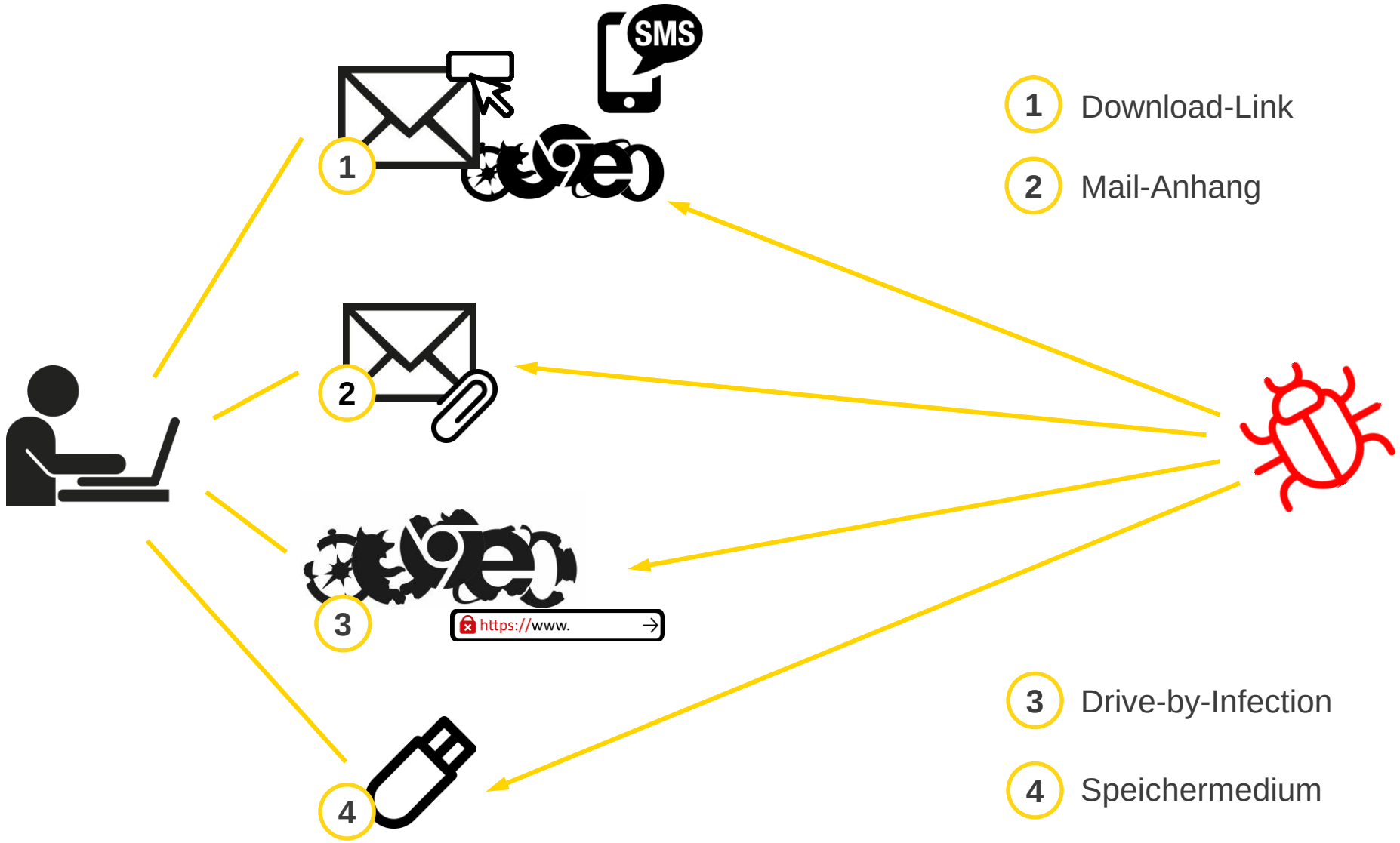


Ausnutzung menschlicher «Schwächen»

- Stress
- Finanzieller Anreiz
- Emotionen
- Neugier
- Ablenkung
- Komplexität
- Hilfsbereitschaft

An erster Stelle steht die Beschaffung von Informationen

Fazit: Achten Sie auf diese Einfallstore



Beispiele aus dem Alltag

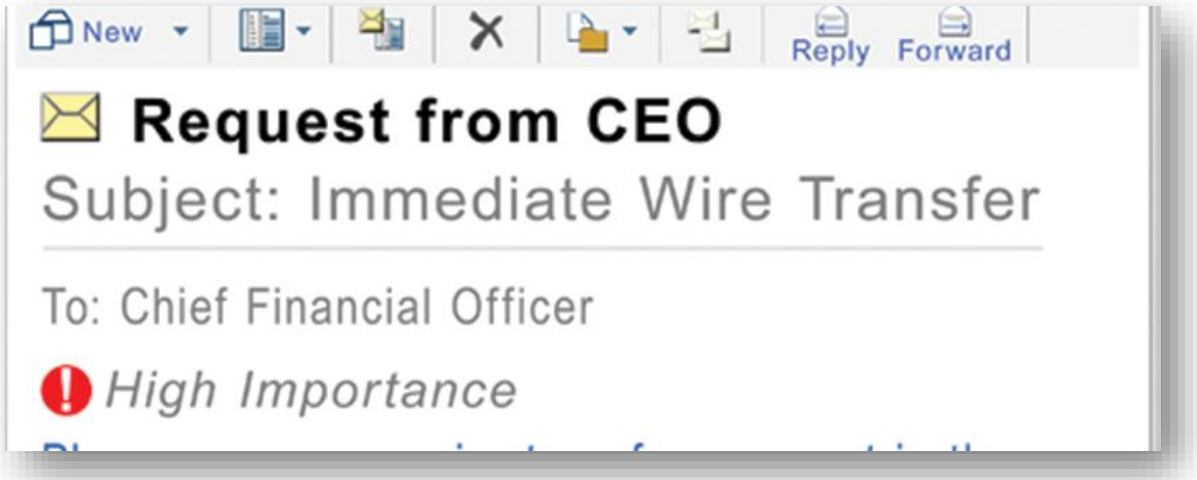
… und wie stark ist IHR Passwort?

Kommen wir als InfoGuard an Hashwerte können wir sie mit Hilfe unserer Infrastruktur knacken. Wie lange würde es dauern?

(Budget ca. 3.500.- «Gaming PC»)

Beispiele aus dem Alltag: «Social Engineering»
Achtung Punk Alarm

Beispiele aus dem Alltag: «CEO Fraud» – Entscheidungsträger im Fokus von Cyberattacken



- Mail von gefälschtem Absender (CEO) an den CFO
- “Bitte überweise 50 TCHF für wichtige Transaktion auf Konto xx.yy.zzzz”
- Vielfach Zeitdruck (Freitag Abend, Deal muss raus, Kunde springt ab, …)
- Konto gehört Angreifer

Beispiele aus dem Alltag: «Ransomware» – Wenn Verschlüsselung zum Albtraum wird

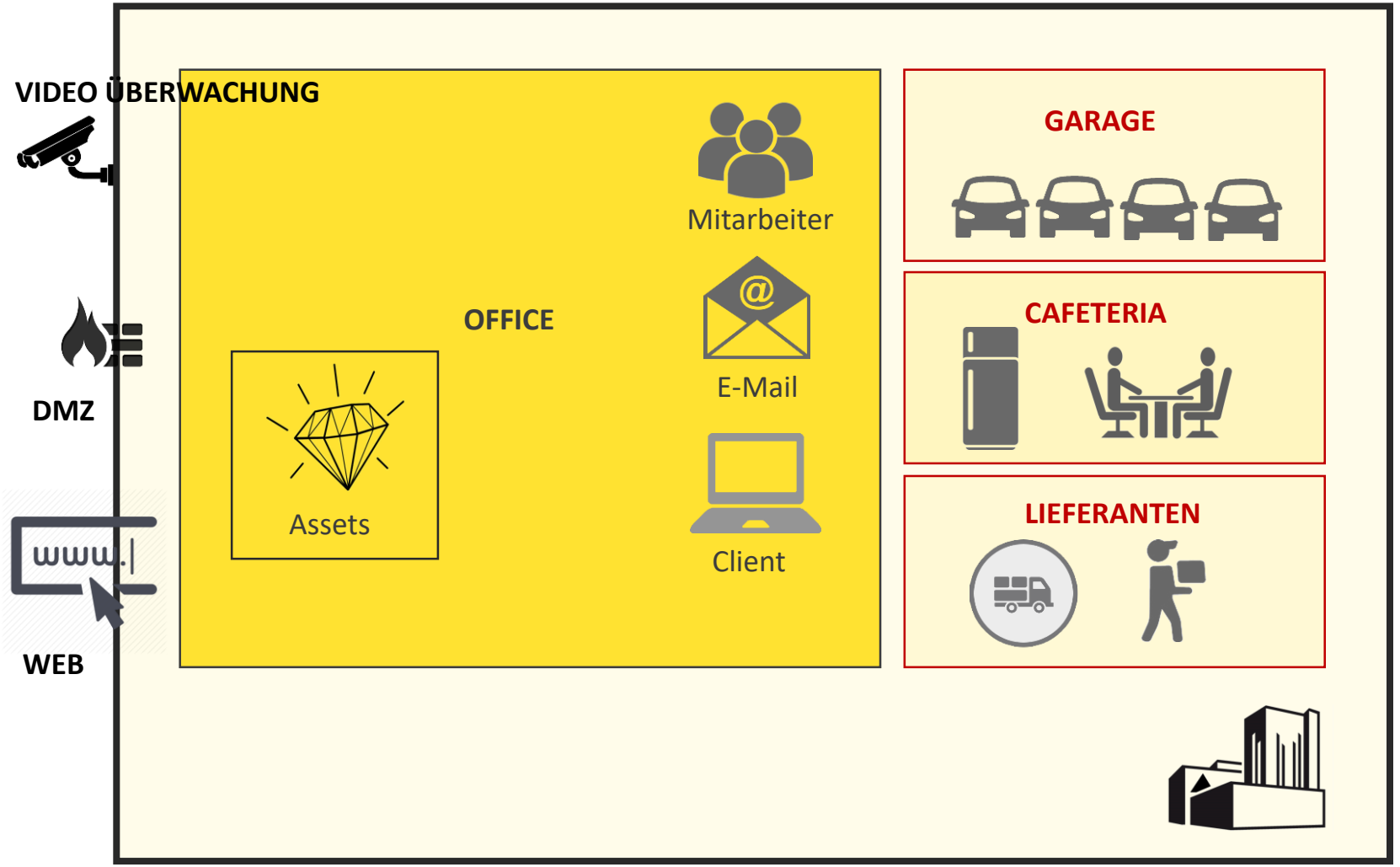
InfoGuard
SWISS CYBER SECURITY

- Ransomware Angriff eines Insiders
- Lösegeldforderung pro Terminal- und Backup-Server
- Keine Office/PDF/IMG Files verschlüsselt, sondern nur Files des Software-Herstellers!
- 150 von 200 Terminal Server (TS) verschlüsselt
- 2 Backups: 1x OK, 1x verschlüsselt
- 90% TS konnten wieder hergestellt werden
- Die wichtigsten Kunden blieben verschlüsselt!

Beispiele aus dem Alltag: «Malware» – Hightech verbreitet Malware

- Medizintech für mehrere Mio $
- NotPetya Malware (06.2017)
  - MS Patch wäre längst verfügbar
- ~150 Systeme infiziert, bevor die Ausbreitung gestoppt wurde
- Glück gehabt!
  - Nur ausgebreitet, aber
  - Nicht verschlüsselt
- Ist der Lieferant für Schaden & Aufwand haftbar?

Beispiele aus dem Alltag: Weiter Potentielle Eintrittsvektoren



Beispiele aus dem Alltag: Third-party risk

- Nearly 70% of Breaches are a Result of Poor Third-Party Security.
- Third parties can be your weakest security link.
- Unfortunately, it’s true even if that weakest link isn’t part of your own organisation.
- If a third party with access to your systems – contractor, partner, supplier—gets breached, well then, you’ve been breached too.

Beispiele aus dem Alltag: Achtung USB Stick

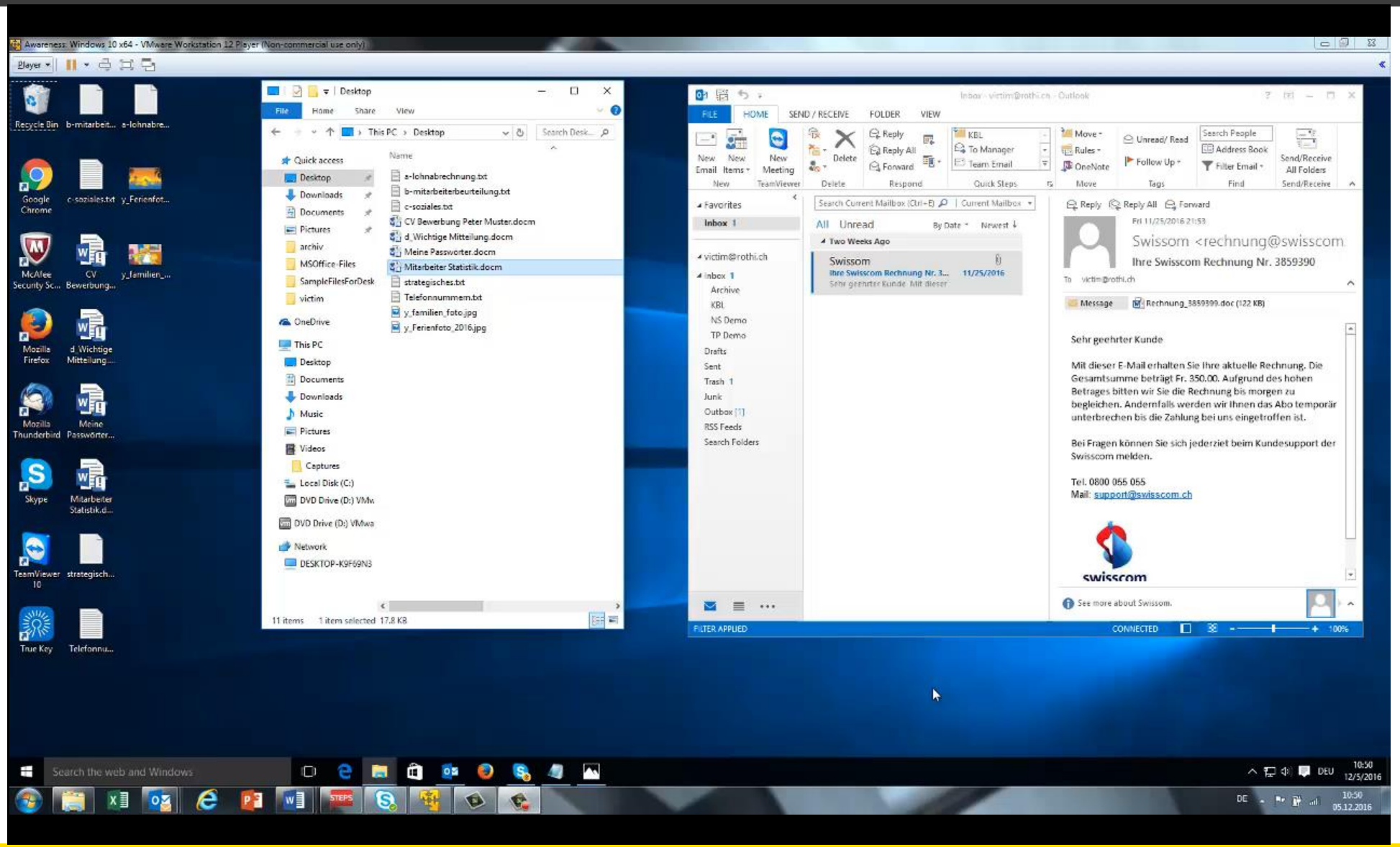
- Der USB Rubber Ducky ist nicht so harmlos, wie er aussieht.
- Am Rechner meldet er sich als USB-Tastatur an und übernimmt ungefragt das Ruder.
- Preis 45 US $

Beispiele aus dem Alltag: Ransomware

Stellen Sie sich vor, …

……Sie verlieren alle Ihre Daten die auf Ihrem Computer gespeichert sind.

Live Demo – Phishing Mail mit Attackment und Verschlüsselung



Tipps & Tricks

Für den Alltag (geschäftlich & privat)

Tipps für den Alltag: Phishing

Bei verdächtigen Mails ist das richtige Verhalten wichtig…

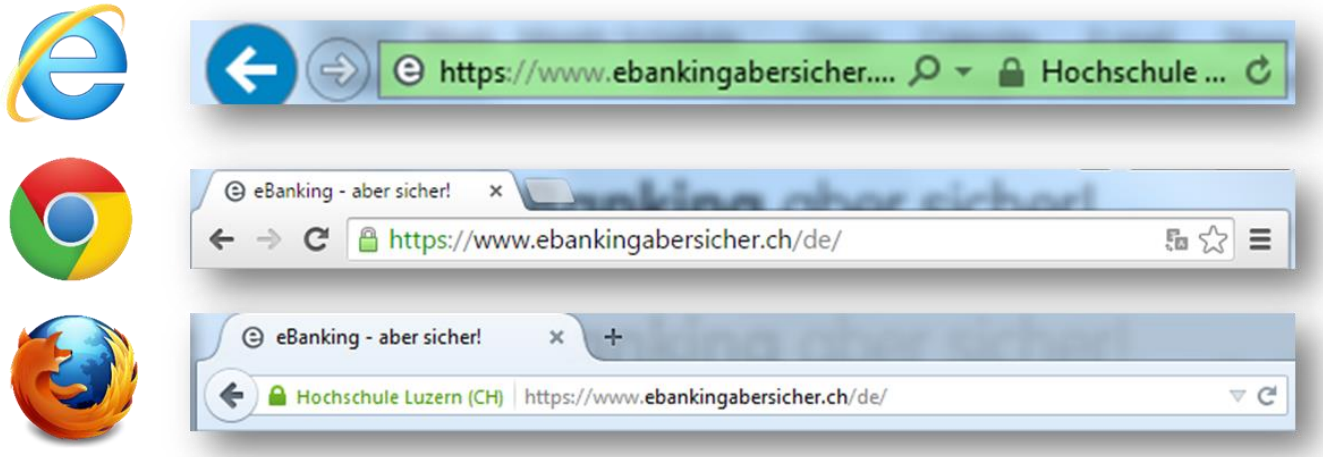
- Überprüfen der Absenderadresse
- Überprüfung des Texts (unverständliche / schlechte Formulierungen, Schreibfehler)
- Achten Sie auf den Link und auf bösartige “Attackments”.

- Ignorieren Sie nicht die Sicherheitswarnungen und aktivieren Sie keine Makros.
- Nachdenken über Plausibilität der Aufforderung etwas bekanntzugeben.
- Passwörter dürfen unter keinen Umstanden über öffentliche Webseiten preisgegeben werden, auch wenn sie auf den ersten Blick echt und „lohnend“ aussieht.
- Vorfall der IT Abteilung / Help Desk melden
- Verdächtige Mails löschen (ungeklickt!)

Tipps für den Alltag: https - Zertifikatsüberprüfung

Regeln: Das Zertifikat ist echt und gültig, wenn ...

- der Browser beim Aufbau der SSL-Verbindung keine Fehlermeldung zeigt.
- am Anfang der Adresszeile «https://» steht.
- ein Schloss angezeigt wird (evtl. verborgen hinter der Schaltfläche zur Webseitenidentität).



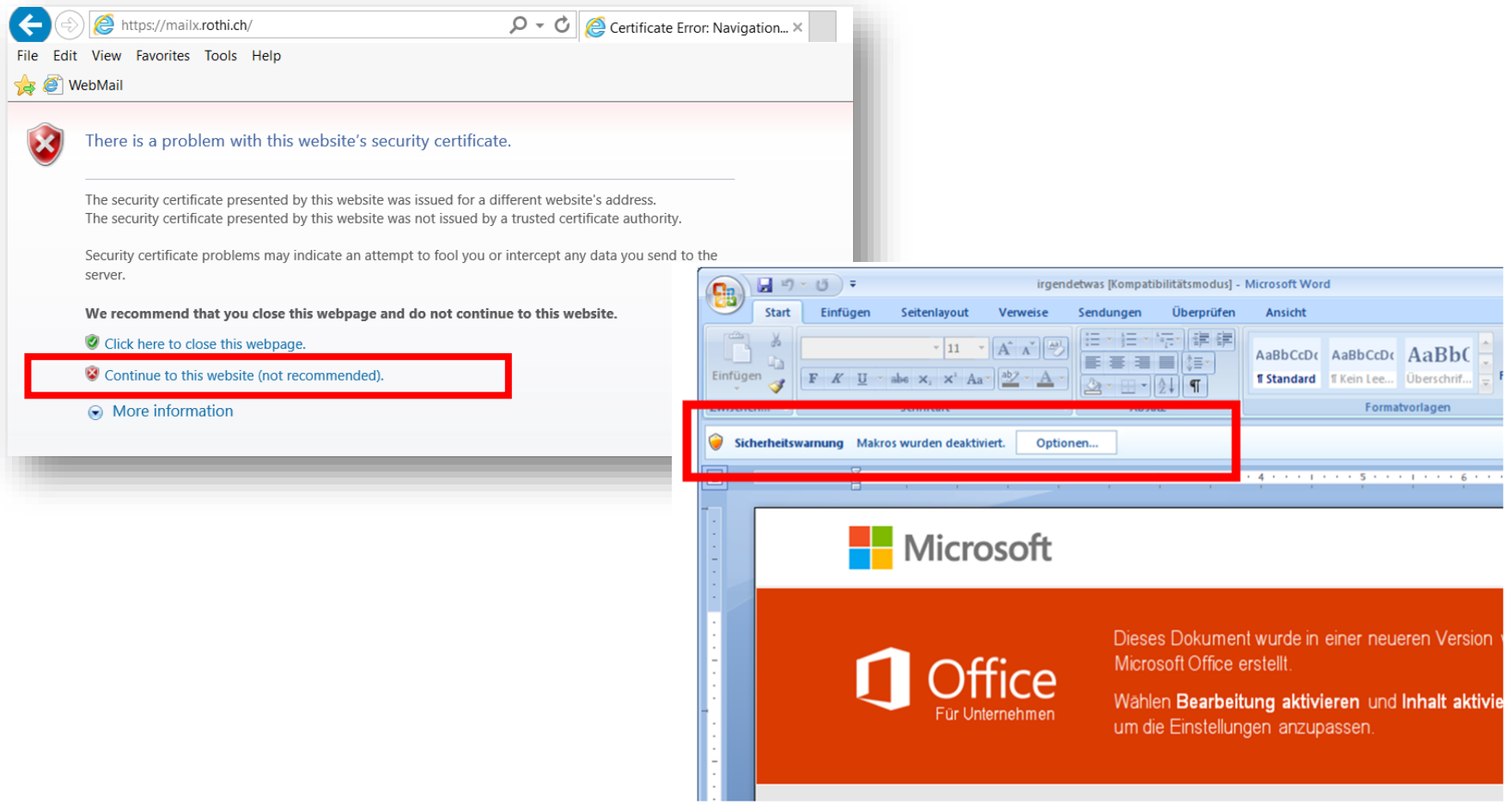
Tipps für den Alltag: Machen Sie Passwörter einfach STARK.

Waliays_TB66!

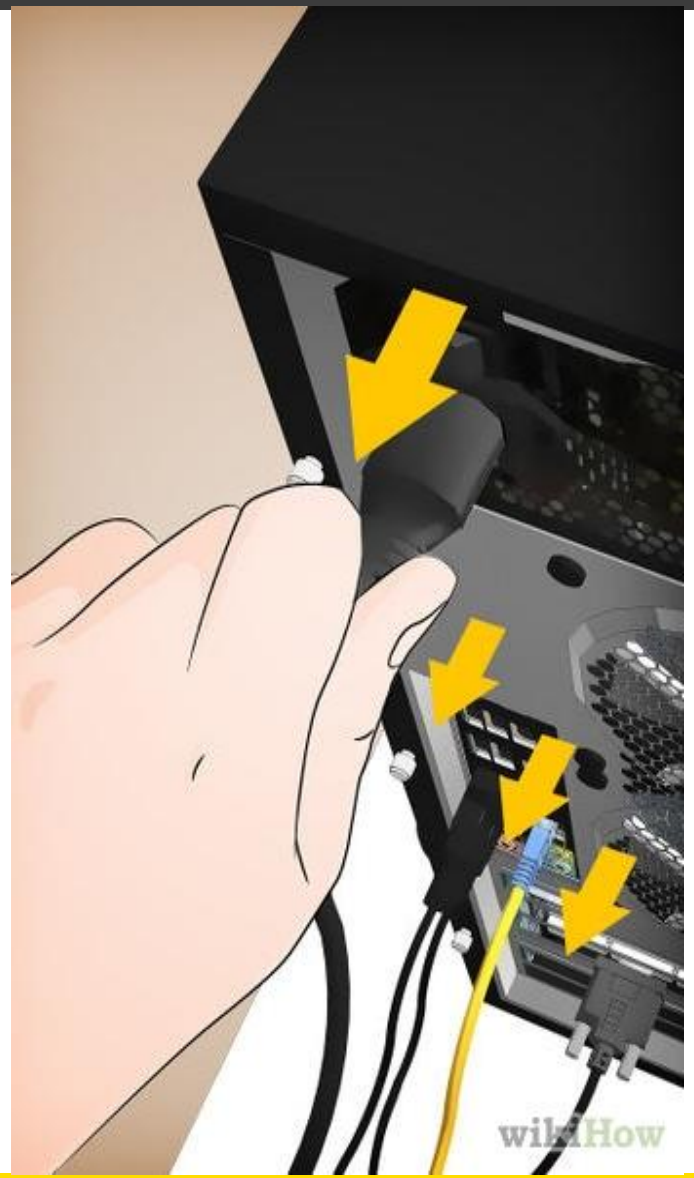
- **Geben** Sie Ihre Passwörter **weder Mitarbeitenden**, noch **Stellvertretungen** oder **Systemverantwortlichen bekannt**.
- **Sperren** Sie Ihren PC **bei Abwesenheit** vom Arbeitsplatz.
- Wechseln Sie Passwörter sofort bei Verdacht auf Missbrauch.
- Benutzen Sie **verschiedene** Passwörter für unterschiedliche Anwendungen.
- Verwenden Sie **geschäftlich** und **privat andere** Passwörter.
- Bewahren Sie Passwörter nur an einem geschützten Ort auf (z.B. Passwortmanager KeePass / SecureSafe).
- Wechseln Sie Initialpasswörter beim ersten Gebrauch.
- Wählen Sie ein **komplexes Passwort** von mindestens 8 Zeichen (Gross- und Kleinbuchstaben sowie Zahlen oder Sonderzeichen)

Tipps für den Alltag - Datendiebstahl

Ignorieren Sie nicht die Sicherheitswarnungen und aktivieren Sie keine Makros.



Tipps für den Alltag - Ransomware



Verhaltensweisen bei einem Ransomware-Befall

- Infizierte Maschine sofort vom Netzwerk trennen
- Informieren Sie den Bereich ICT
- Nicht bezahlen!
- Infizierte Maschinen durch neue ersetzen
- Backup wiederherstellen

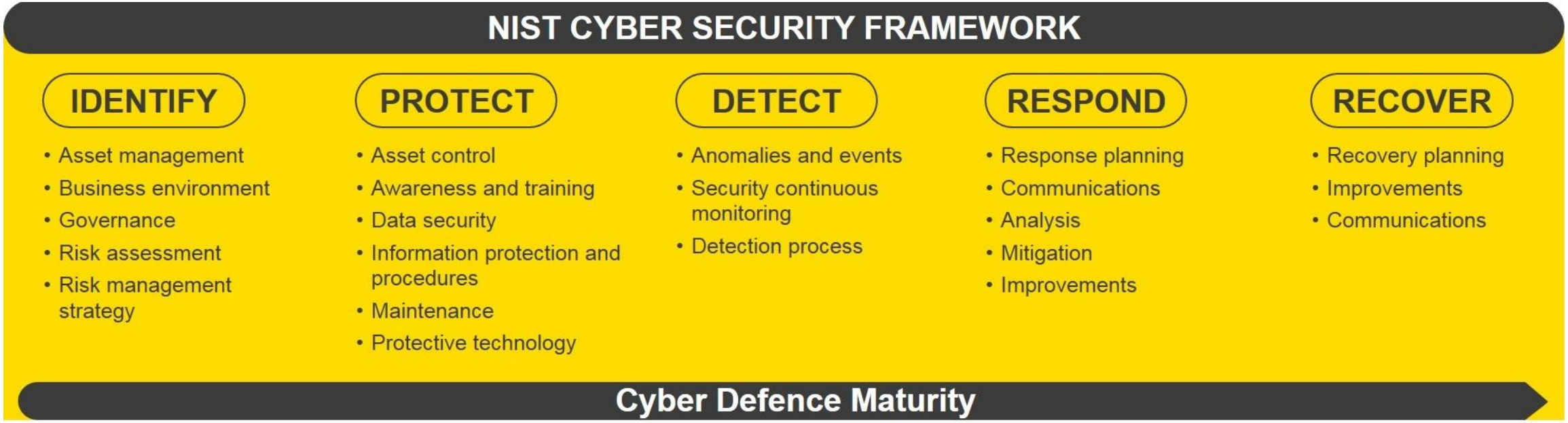
Tipps für den Alltag: USB Memory Stick

InfoGuard
SWISS CYBER SECURITY

Finger weg von USB-Sticks unbekannter Herkunft:

- Die Anti-Viren-Software wird nicht anspringen und es ist für den Besitzer des USB-Sticks ein leichtes Spiel ist, Passwörter und andere sensible Daten auszuspionieren.
- Öffnen von Dokumenten: Öffnen Sie keine Dokumente ohne dass der USB Memory Stick vorher getestet wurde. Bringen Sie den USB Memory Stick einer Fachperson zum testen (IT Abteilung).
- Unbekannte Herkunft: Sind Sie vorsichtig bei gefunden und zugestellten USB Memory Stick (Bewerbungen, Werbegeschenke, etc.). An einen Rechner sollten Sie kein USB Memory Sticks anschliessen, dessen Herkunft Sie nicht kennen.
- Ohne Aufsicht: Wenn ein USB Memory Stick kurz unbeaufsichtigt ist oder verloren geht, könnten Daten manipuliert werden.

Cyber Security Strategie – Security Frameworks



Verschiedene Security Frameworks wie ISO, Grundschutz, NIST geben Auskunft darüber, welche Standards und Best Practices in Ihrem Unternehmen umgesetzt werden müssen, um Cyber Risiken effektiv zu steuern und die Cyber Risiken zu minimieren.

Persönlicher Grundschutz gilt auch für zu Hause

- **Aktualisieren** Sie Ihre Software und OS regelmässig.
- Sichern Sie Ihre Daten regelmässig mit **Backups**
- Nutzen Sie ein Antivirus-Programm mit Webfilter und halten Sie dieses aktuell
- Schützen Sie Ihren Internetzugang mit einer Personal-Firewall
- Verwenden Sie **starke und unterschiedliche Passwörter** oder wenn möglich sogar eine Zwei-Faktor-Authentisierung
- Schützen Sie Ihre mobilen Geräte mit einem **PIN**
- Ignorieren Sie NICHT die Sicherheitswarnungen und aktivieren Sie keine Makros.

Fragen und Diskussionen