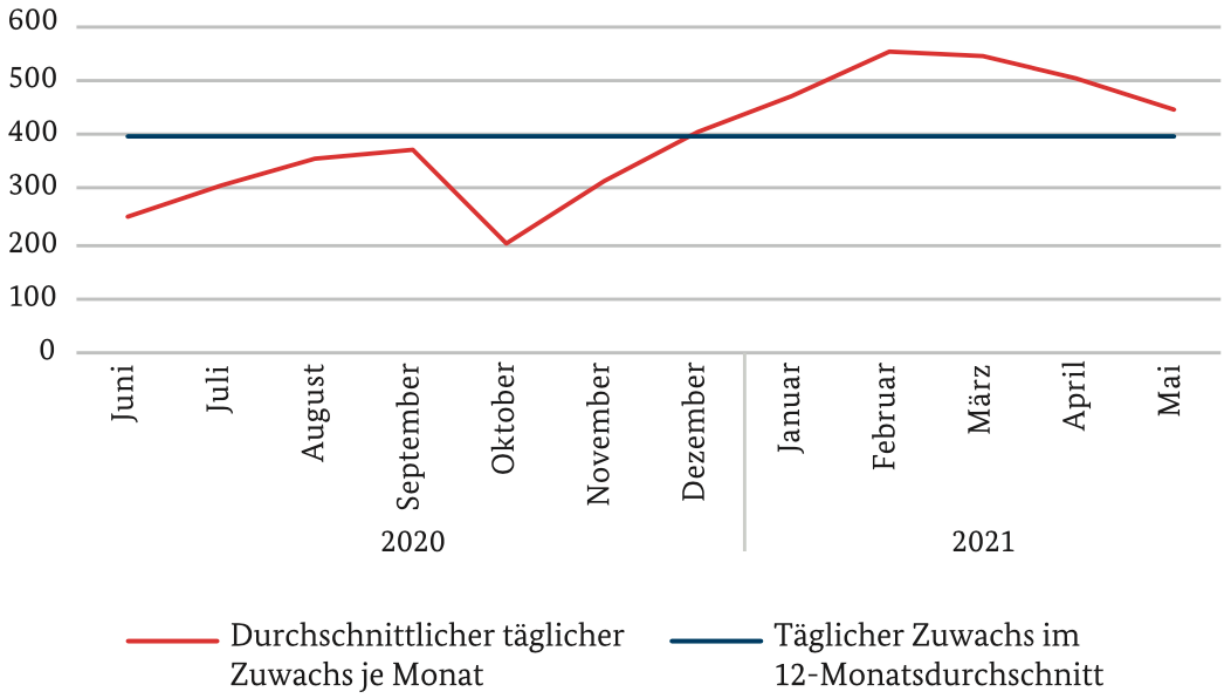
Aktuelle Bedrohungen der Informationssicherheit

Alles nur Räubergeschichten?

Viele neue Schadprogramme

- Die Anzahl neuer Schadprogramm-Varianten (neuer Hashwert) liegt bei hunderten Millionen pro Jahr
- Im Februar 2021 wurde mit **durchschnittlich 553.000 neuen Varianten (Mutationen) pro T**ag der höchste jemals gemessene Tageszuwachs an neuer Schadsoftware verzeichnet



Quelle: BSI Lagebericht 2021

Ransomware Angriffe

- Hacker haben bisher im Jahr 2022 (Stand August) bei 320 Vorfällen mehr als 30 Terabyte (TB) an persönlichen und anderen sensiblen Daten gestohlen
- Die Gesamtzahl der globalen Ransomware-Angriffe beläuft sich im Jahr 2021 auf fast 20 Versuche pro Sekunde.
  - Die USA sind mit 421,5 Millionen Ransomware-Angriffen am meisten betroffen.
  - 2021 gab es 34,2 Millionen Ransomware-Angriffe in Deutschland und 33,5 Millionen im Vereinigten Königreich.
  - Für Österreich liegen keine aktuellen Statistiken vor.

Quelle: https://atlasvpn.com/blog/ransomware-hackers-drained-over-30-terabytes-of-sensitive-data-in-2022
Quelle: https://atlasvpn.com/blog/ransomware-volume-doubles-in-2021-surpassing-600-million

Advanced Persistent Threats

- APTs oft langfristig und mit großem Aufwand geplante Angriffe auf einzeln ausgewählte, herausgehobene Ziele.
- APT-Angriffe dienen nicht primär der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und ggf. der Sabotage.
- Die meisten E-Mail- basierten Angriffe als Bestandteil von APTs nutzen keine technischen Schwachstellen. Stattdessen wird die Anwenderin bzw. der Anwender dazu verleitet, Warndialogfenster zu ignorieren und Makros und andere schädliche Inhalte auszuführen.
- Der überwiegende Teil der APTs richtet sich an Regierungsbehörden.

information security consulting
Beratung - Ermittlung - Schulung

Identitätsdiebstahl nimmt zu

eDAY22
Mi., 14. September 2022

- Aktuelle **Phishing-Kampagnen** adressieren gesellschaftliche Ereignisse und aktuellen Themen, wie etwa die COVID-19 Pandemie und damit zusammenhängende Förderungen oder Steuererleichterungen.
- Online-Händler stehen aufgrund der auf ihren Websites verarbeiteten Kundendaten immer wieder im Fokus von Angriffsbemühungen durch **Skimming**.
  - Bei Web-Skimming-Angriffen werden legitime Webseiten von Online-Händler kompromittiert, teils ohne dass die Betreiber der Plattformen dies direkt bemerken.
- Cyber-Angriffe auf **Videokonferenzen**
  - Beim sogenannten Credential Stuffing werden Nutzerdaten aus vorangegangenen Daten-Leaks automatisiert bei verschiedenen Videokonferenzanbietern ausprobiert, um zu testen, ob auch damit eine Anmeldung möglich ist.

Schutzgelderpressungen

- Als **Denial-of-Service**-Angriffe (DoS-Angriffe) werden Überlastungsangriffe auf Internetdienste bezeichnet.
- Ziel der Angriffe sind oft Service Provider und Webshops. Dabei wird immer wieder folgende Vorgangsweise beobachtet:
  - Der initiale Kontakt erfolgt mit einer **Erpressungs-E-Mail**, in der ein bevorstehender DDoS-Angriff auf das Unternehmen angekündigt wird, falls eine Schutzgeldforderung (meistens in Bitcoins) innerhalb einer genannten Frist nicht gezahlt wird.
  - Für den Fall, dass den Lösegeldforderungen nicht nachgekommen wird, werden Angriffe von über 2 Tbit/s angedroht. Zuletzt wurden derartige Angriffe bei der **Erpressung der neuseeländischen Börse NZX** tatsächlich umgesetzt.

Quelle: https://www.handelsblatt.com/technik/thespark/new-zealand-exchange-cyber-angriffe-legen-boersenhandel-in-neuseeland-dritten-tag-in-folge-lahm/26132196.html

Angriffe auf Verschlüsselung

- Die Frage ist nicht ob sondern wann die derzeit bestehenden starken Verschlüsselungssysteme geknackt werden können
- Der aktuelle Standard RSA (benannt nach den Anfangsbuchstaben der Nachnamen der Kryptographen Ronald Linn Rivest, Adi Shamir und Leonard Max Adleman) ist aktuell noch sicher
  - Ein internationales Forscherteam vermeldet jedoch Erfolge beim Knacken der Verschlüsselung. Sie verkündeten, dass sie die RSA-240-Challenge gelöst haben, was das Knacken eines RSA-Schlüssels mit 795 Bit bedeutet. Die letzte RSA-Challenge mit 768 Bit wurde vor zehn Jahren gemeistert.
  - RSA mit 1024-Bit-Schlüsseln sind zwar immer noch nicht geknackt, aber die Uhr tickt.
  - **Mittelfristig sollte man keine Schlüssel unter 4096 Bit mehr benutzen**.

information security consulting

Beratung - Ermittlung - Schulung

Krieg in der Ukraine

eDAY22 Mi., 14. September 2022

- Experten von Microsoft haben seit Beginn des russischen Angriffskriegs gegen die Ukraine **Attacken russischer Hacker auf 42 Länder** festgestellt
  - Insgesamt sind bis heute mindestens 128 Organisationen betroffen
- Die Ukraine hat die Angriffe abgewehrt, indem sie große Teile ihrer digitalen Infrastruktur in die Cloud verlegt hat
- Die USA sind das wichtigste Ziel – bekannt wurden aber auch Cyberangriffe auf Polen, die baltischen Staaten, Dänemark, Norwegen, Finnland, Schweden, die Türkei und andere NATO-Länder

Quelle: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Hybride Angriffe

- Hybride Bedrohungen bezeichnen verschiedene Formen **illegitimer Einflussnahme durch fremde Staaten**
  - Ein Beispiel für Angriffe im Sinne hybrider Bedrohungen sind Cyberangriffe, mit denen sensible Informationen rechtswidrig abgegriffen werden, um diese in einem zweiten Schritt manipulativ zu verbreiten und so im Informationsraum mittels Diskreditierung oder Desinformation schädliche Wirkung zu entfalten.
  - Beispielsweise wurde durch Cyber-Angriffe und Desinformationen europäische Impfkampagnen zu beeinflusst. So wurde die Europäische Arzneimittelagentur EMA Ziel eines Cyber-Angriffs. Abgeflossene COVID19 Studien wurden durch die selektive Verbreitung dazu benutzt, die öffentliche Meinung in illegitimer Weise zu beeinflussen und **Falschbehauptungen zu Impfungen** Vorschub zu leisten

Quelle: https://www.golem.de/news/corona-impfstoffe-europaeische-arzneimittelagentur-ema-gehackt-2012-152726.html

Aktuelle Vorfälle

- Erneuter Datendiebstahl von Kundendaten bei Samsung (8.9.2022)
- Cyberangriff beschäftigt Wasserzähler-Hersteller Ista (22.8.2022)
- 405 Mio Strafe für Data Breach von Kinderdaten bei Insta (6.9.2022)
- Angriff auf Kärnten - 80.000 Stammdatenblätter ausgelesen (Juli 2022)
- Hacker stellt Kundendaten von Zurich Versicherung online (Nov 2021)
- CCC meldet 6,4 Millionen Datensätze in über 50 Leaks (April 2022)
- …
- …

Aktuelle Publikationen auf der Homepage des des Bundesministeriums für Finanzen und des A-SIT Zentrum für sichere Informationstechnologie https://www.onlinesicherheit.gv.at/Services/Publikationen.html

information security consulting

Beratung - Ermittlung - Schulung

Herausforderung DSGVO

eDAY22 Mi., 14. September 2022

- Längst nicht nur mehr multinationale Konzerne wurden auf Grund unzureichender **technischer und organisatorische Maßnahmen** zur Gewährleistung der Informationssicherheit zu empfindlichen Geldstrafen verurteilt
- Die neuen gesetzlichen **Dokumentations- und Meldepflichten**, etwa in Hinsicht auf Datenschutzverletzungen, sind noch längst nicht in der Breite bekannt.
- Unter https://www.enforcementtracker.com findet sich eine aktuelle Übersicht auf welcher nach Ursache und Strafhöhe gefiltert werden kann
- Die WKO stellt gute Informationen über die effektive und effiziente Umsetzung von technisch organisatorischen Maßnahmen (TOM) zur Verfügung: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

Alles nur Räubergeschichten?

Lösungsansätze

- Cybersecurity ist eine Führungsaufgabe und funktioniert nur im **Verantwortungsbereich der Unternehmensführung**
- Das Rad muss nicht neu erfunden werden, orientieren Sie sich an best practices (z.B. ISO 2700x).
- Innerhalb eines Information Security Management Systems (ISMS) sind **Regeln, Verfahren, Maßnahmen und Tools** zu definieren, mit denen sich die **Informationssicherheit steuern, kontrollieren, sicherstellen** und **optimieren** lässt.
- **Durch die IT verursachte Risiken sollen identifizierbar und beherrschbar werden.**

Danke für Ihre Aufmerksamkeit

Michael Mrak

i.s.c. Group
Head of Data Protection Services

Mail: mmrak@iscgroup.co.at
Mobile: +43 664 5032331
https://www.iscgroup.co.at

https://www.linkedin.com/in/michaelmrak/