kantonschwyz

IT-Sicherheit für Unternehmen und Privatpersonen

Stefan Heinzer, Vorsteher Amt für Informatik, stefan.heinzer@sz.ch

Agenda

- Öffentliche Wahrnehmung
- IT-Sicherheit generell
- IT-Risiken
- Problempunkte Risikominimierung CyberCrime
- Organisationen z.B. MELANI (Melde- und Analysestelle Informationssicherung)
- Tendenzen
- Empfehlungen

Öffentliche Wahrnehmung – Oktober 2016

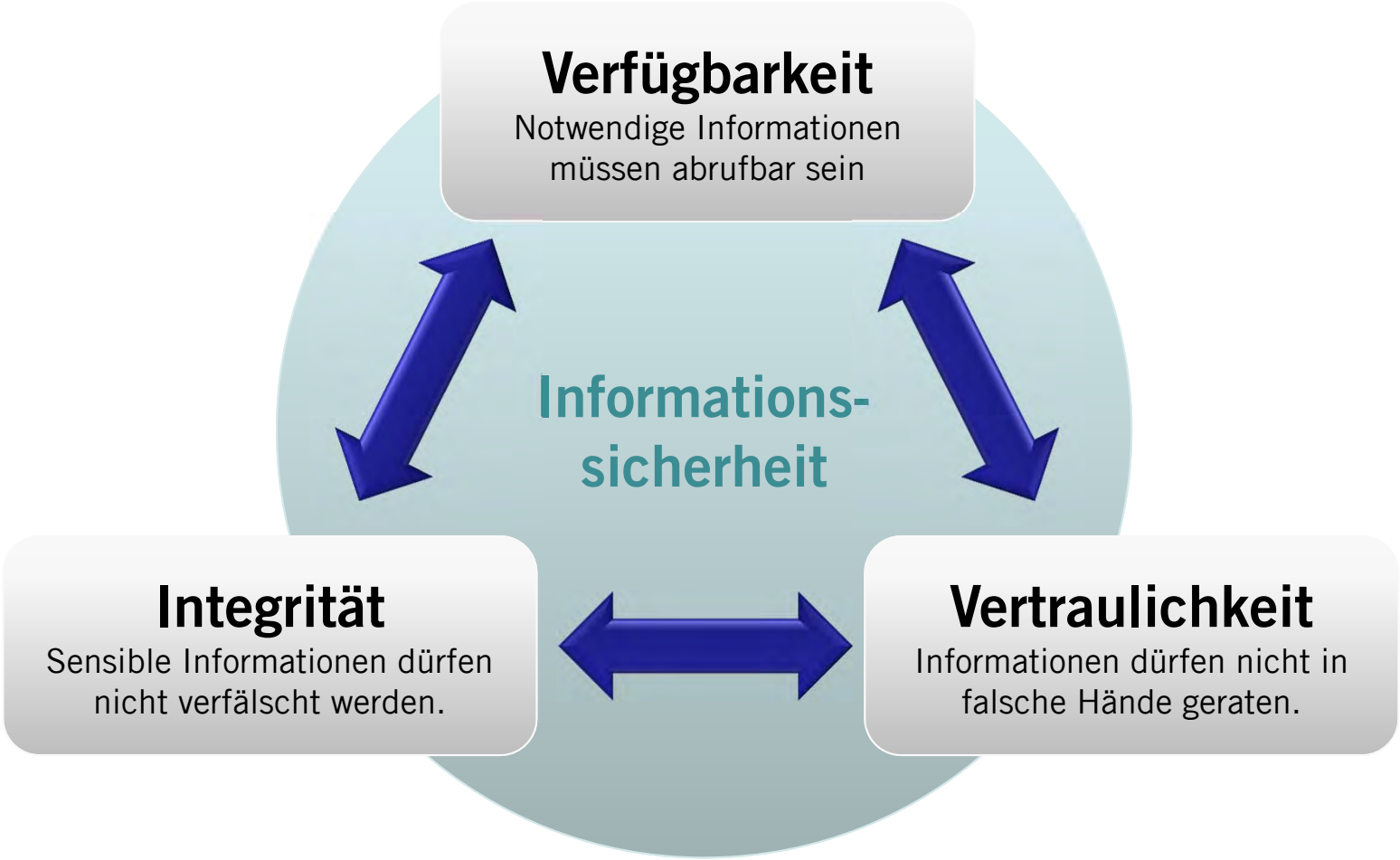
Öffentliche Wahrnehmung – Mai 2017 (Wanna Cry)

kantonschwyz

Öffentliche Wahrnehmung – Juni 2017 (NotPetya)

- Angriff auf gleichen Sicherheitsmängeln wie Wanna Cry
- Scheinbare Unterlassungen bezüglich Patchmanagement öffentlich diskutiert
- Kompromittierte Systeme nicht einfach erkennbar → Behandlung aufwendig und kompliziert

IT-Sicherheit generell



Konsequenzen:
- Unterbruch der Geschäftsprozesse
- Projekt-Verzögerung
- Verlust von vertraulichen Daten oder Know-how
- Bussen (juristische Konsequenzen)
- Image Schaden
- Wiederherstellungskosten

IT-Risiken

Höhere Gewalt

Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …

Menschliches Versagen

Bedienungsfehler, Unwissen, falsches Verhalten, …

Gesetzliche Mängel

Nicht Einhalten der Gesetze, Reglemente etc. (Compliance)

Technisches Versagen

Netzwerkausfall, Software-Fehler, Disk-Ausfall, …

Organisatorische Mängel

Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …

Vorsätzliche Handlungen

Manipulation, Phishing, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

kantonschwyz

Problempunkte erfolgreicher Risikominimierung des CyberCrime

- **Virtuelle vs. Physische Welt** → Umgang mit digitalen Identitäten
- **Fehlende organisatorische Vorgaben** → Datenklassifikation, Prozessbeschreibungen
- **Stärkung der Präsenz der Informatik** → «Internet of Things», Digitalisierung
- **Verwischung der Sicherheitsperimeter** → «Bring your own Device» / Cloud-Services
- **Ungleichgewicht Ressourcenbedarf «Angriff <-> Verteidigung»** →7x24h-Erwartungshaltung vs. (zahlbarem) Servicebetrieb / Komplexität der Angriffe
- **Erschwerte Strafverfolgung** → Nationale Gesetze versus international organisierten Straftätern
- **Kommerzialisierung CyberCrime** → Shodan-Suchmaschine für Sicherheitslücken

Organisationen im CyberCrime-Umfeld → MELANI (www.MELANI.admin.ch)

Melde- und Analysestelle Informationssicherung MELANI

In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

Die Website von MELANI richtet sich an private Computer- und Internetbenutzer, sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz. Viren und Würmer haben in der Vergangenheit bereits Millionen von Computern lahm gelegt. Die entstandenen Schäden wie Datenverlust oder Ausfall von Dienstleistungen waren riesig. Das muss nicht sein! Schützen Sie Ihre wertvollen Daten!

Informationen für:

INFO

Dokumentation

DOKU

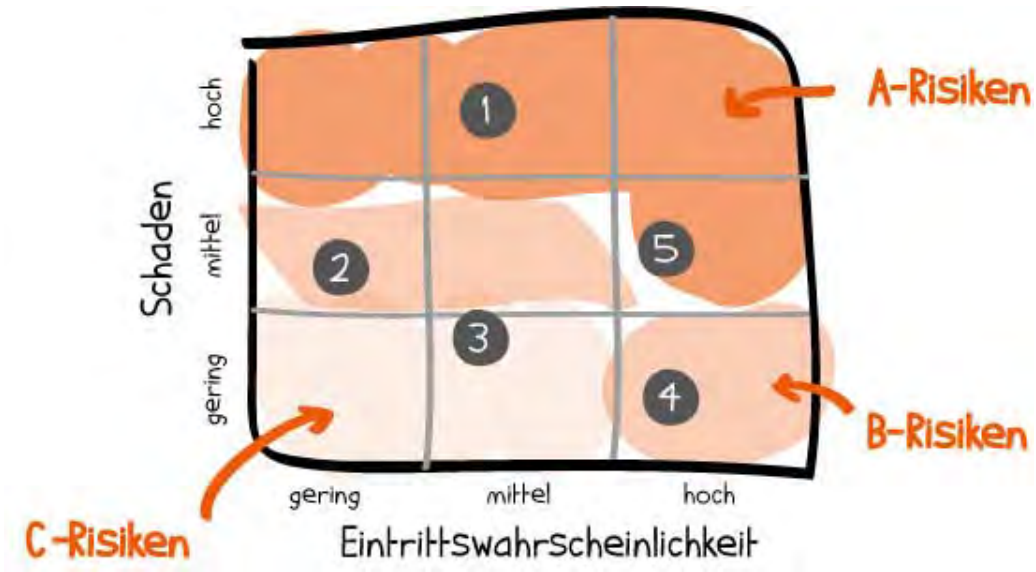
Die MELANI Halbjahresberichte erläutern die wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in den Informations- und Kommunikationstechnologien (IKT). Mit Checklisten und Anleitungen können Sie in verschiedenen Themenbereichen Ihre Systeme sicherer machen.

IT-Risiken Tendenzen

Risiko	Tendenzen / Risikobarometer	
Höhere Gewalt	Klimawandel, Privatisierung Strommarkt, SmartGrid	
Menschliches Versagen	Höhere Anforderungen durch stärkere Vernetzung und steigende Abhängigkeiten, Umgang mit digitaler ID	
Gesetzliche Mängel	Steigende Compliance-Anforderungen, neue Datenschutzgesetze	
Technisches Versagen	Stärkung von Redundanzen / höhere Zentralisierung	
Organisatorische Mängel	Je nach Organisation	
Vorsätzliche Handlungen	Steigende Professionalisierung CyberCrime, stärkere Vernetzung der Systeme, BYOD	

kantonschwyz

IT-Risiken Empfehlungen – Aktive Bewirtschaftung Risikoportfolio



- Erkennen/Definieren der Risiken hinsichtlich **Schadenpotential** und **Eintretenswahrscheinlichkeit**
- Definieren **risikomindernden** Massnahmen
- Bereitstellung notwendiger **Ressourcen** oder **Akzeptanz** des Riskolevels

➔ **Sicherheit ist Chefsache**
Unternehmensleitung zusammen mit Technikpersonal

IT-Risiken Empfehlungen – Aufbau «Business Continuity Management»

- **IT-Ausfälle** können trotz aller Massnahmen eintreten
- Vorgängig definierte **Notfallprozesse** inklusive Zuständigkeiten sparen Zeit und Geduld
- Zusätzlich erfolgt eine **Rückkopplung mit der Risikobetrachtung** → allenfalls werden Risiken neu eingestuft
- **Unterschiedliche Rollen/Aufgaben**
  - IT-Systemwiederherstellung
  - Notfallbetrieb
  - Kommunikation intern
  - Kommunikation extern
  - .....

kantonschwyz

IT-Risiken Empfehlungen

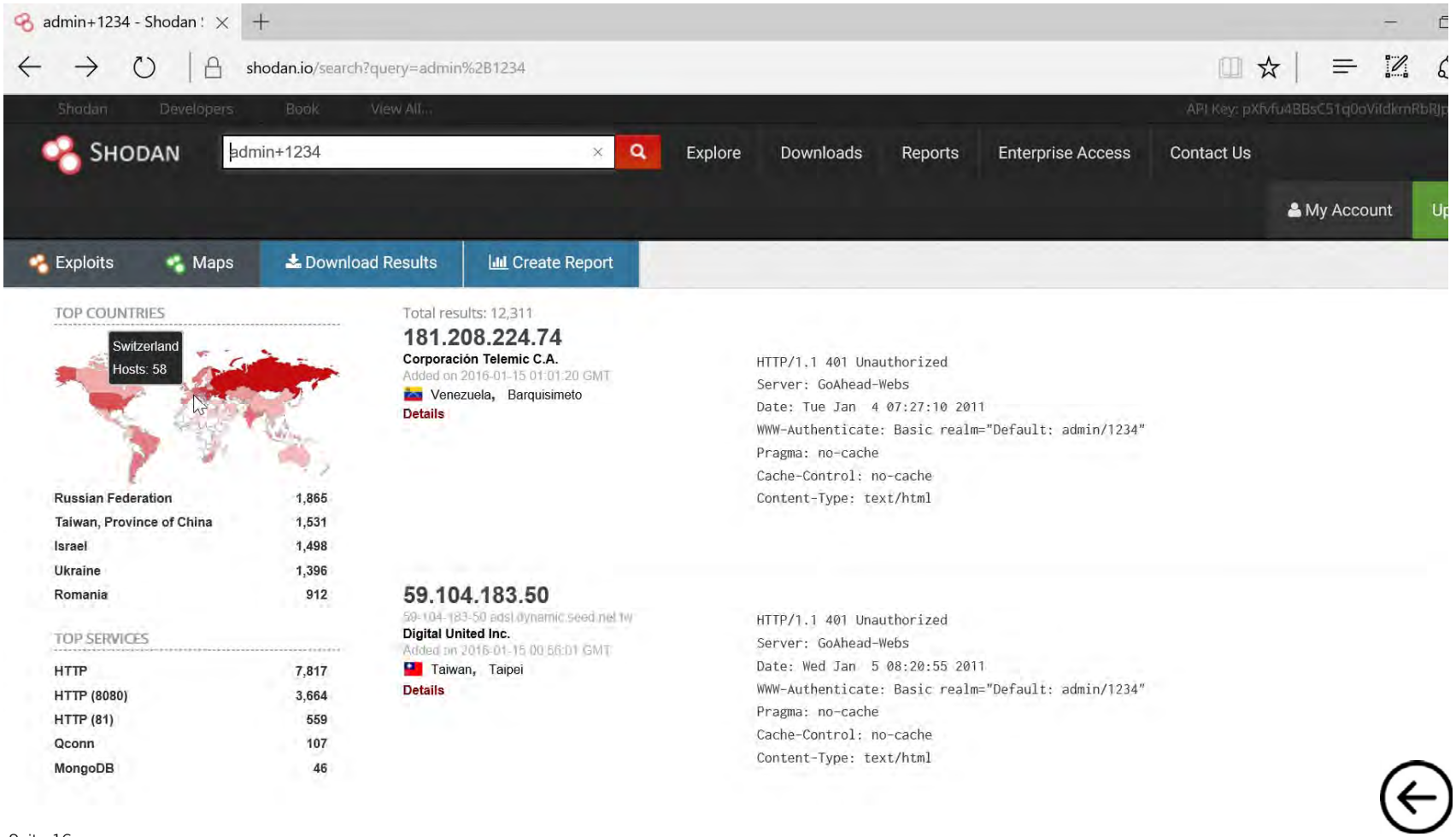
Starten Sie heute....

kantonschwyz

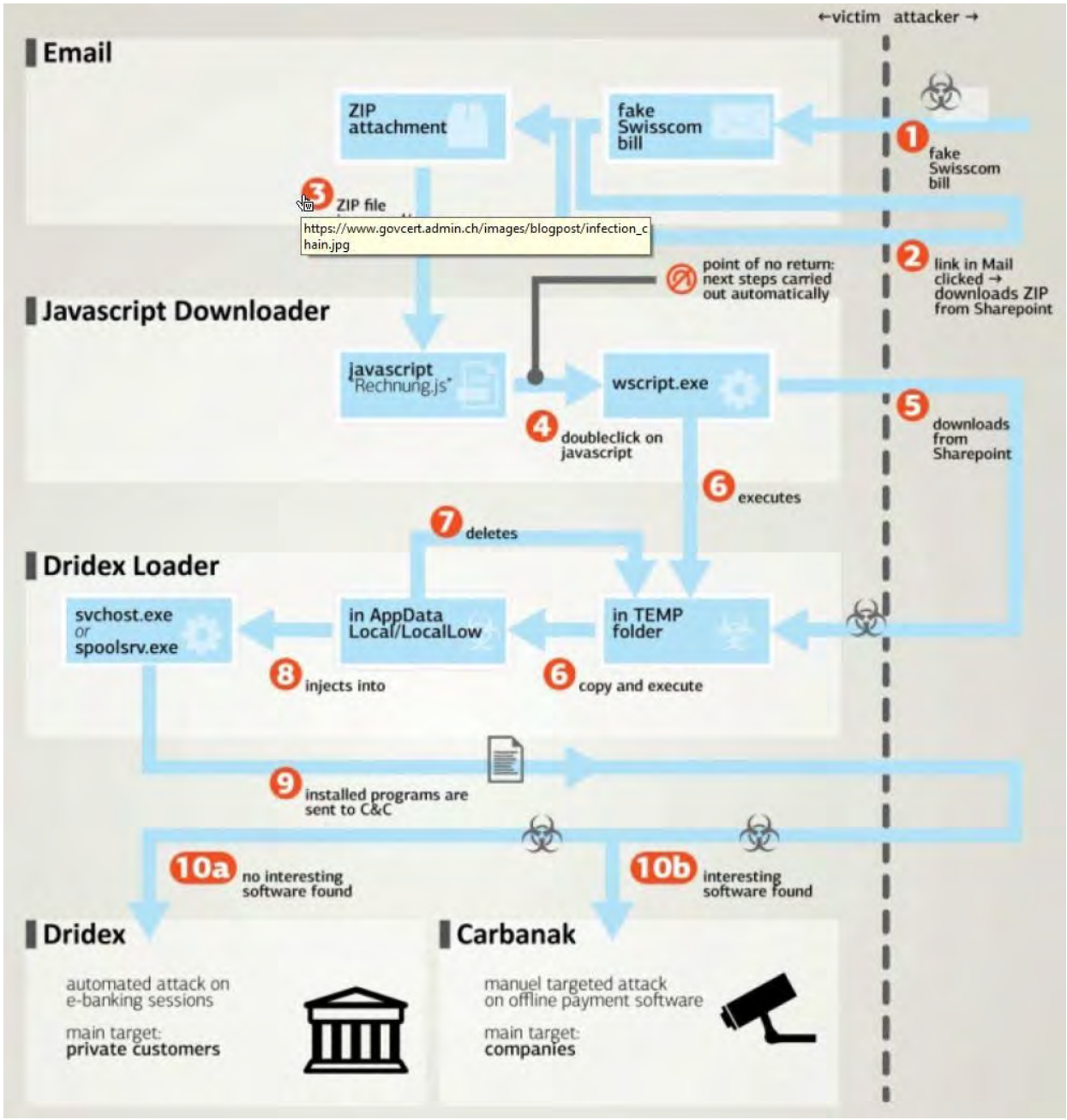
Fragen / Bemerkungen

Anhänge

Shodan Suchmaschine



Komplexität eines Virenbefalls via E-Mail



Fakten Sicherheitsgefährdung (Umfrage IBM)

48% Gefährdung erfolgt durch privilegierte Insider, Administratoren

41% Gefährdung über Social Media

38% Hintertüren, versteckte Funktionen welche bei der Entwicklung von Produkten bereits beim Hersteller einfliessen (Firm-, Middleware, Tool Kits, etc.)

38% Malware, Sicherheitslücken in Produkten (Software, Hardware)

36% Hochentwickelte anhaltende Angriffe gegen die Unternehmung

35% Gefährdungen durch verlorene, gestohlene Geräte

36% Gefährdung durch die Mobilität der Mitarbeitenden und den Einsatz von BYOD

30% Gefährdung spezifisch durch Cloud Computing

243 TAGE Median der Anzahl Tage bis ein gezielter Angriff entdeckt wurde

63% der Angriffe wurden durch Drittparteien festgestellt

>75% der IT und Security Experten sagen, dass langjährige bewährte Technologien zunehmend ineffektiv werden

Quellen: M- Trends 2015, IBM X-Force Report Q 2 2015

kantonschwyz

Mittel zur Risikominimierung ....

(McAfee Labs Threats-Report Juni 2017)

- Erstellen Sie starke Kennwörter und ändern Sie sie regelmäßig.
- Verwenden Sie für jedes Konto und jeden Dienst ein anderes Kennwort.
- Nutzen Sie Möglichkeiten zur mehrstufigen Authentifizierung.
- Verwenden Sie für Aufgaben, die ein Kennwort erfordern, niemals einen öffentlichen Computer.
- Seien Sie beim Öffnen von E-Mail-Anhängen besonders vorsichtig.
- Sorgen Sie auf allen Geräten für einen umfassenden Schutz.

Allgemeine Empfehlungen von MELANI

- Verhaltensregeln
  - Passwort (Länge, Merkbarkeit, keine Mehrfachverwendung)
  - E-Mail (unbekannte Absender, Vertrauenswürdigkeit der Quelle, Verwendung der E-Mailadresse ….)
  - Surfen (Unbekannte Programme, Softwarequelle, Nutzung Social Media…)
  - Peer2Peer (Tauschbörsen)

- Software und Einstellungen
  - Regelmässig Updates (Patches)
  - Personal Firewall, Freigaben
  - Antivirenprogramm
  - Backup (Offline-Zugriff)

- Geräte / Peripherie
  - Ändern Standardpassworte

kantonschwyz

Zusatzinfo WannaCry

- Basiert auf einem Exploit einer Sicherheitslücke im SMB-Protokoll von Microsoft.

- Der US-amerikanische Auslandsgeheimdienst **NSA nutzte diese Lücke über mehr als fünf Jahre, ohne Microsoft über sie zu informieren**, für eigene Zwecke mit einem Exploit, der den Namen EternalBlue erhielt und von Hackern der vermutlich NSA-nahen Equation Group entwickelt worden war.**Erst nachdem die NSA erfahren hatte, dass das Wissen über EternalBlue gestohlen worden war, informierte sie Microsoft über die Sicherheitslücke.**

- Microsoft stellte daraufhin am 12. März 2017 einen Sicherheits-Patch für den SMBv1-Server zur Verfügung, damals allerdings nur für noch von Microsoft unterstützten Betriebssysteme Windows Vista, Windows 7, Windows 8.1 und Windows 10 sowie für Windows Server 2008 und jünger.

- Einen Monat nach den Updates durch Microsoft wurde EternalBlue von der Hacker-Gruppierung The Shadow Brokers öffentlich gemacht.

Begriffe der Internetkriminalität

- **BOT**: (Von englisch robot ‚Roboter') Computerprogramm, das weitgehend automatisch sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein.

- **Exploit**: (englisch to exploit ‚ausnutzen') In der elektronischen Datenverarbeitung eine systematische Möglichkeit, Schwachstellen auszunutzen, die bei der Entwicklung eines Programms entstanden sind.