Botnetze:

→ Botnetze sind ein zusammenschluss mehrer Computer, diese wurde meist Infiziert durch eine “hacker”, dieser kontrolliert alle Infizierten Computer und schickt millionen von Anfragen an einen Host, meist sind dies Serverfarmen, das Ziel dieser Angriffe sind die Lahmlegung des Netzes und die damit entstehenden Kosten bzw. Nichterreichbarkeit der Server

→ Infiziert wird man meist durch E Mails, deren Anhang infiziert ist

Potenziell unerwünschte Programme(PuP) sowie Falsche Antivirensoftware:

→ Erkennung dieser Flachen Software ist bei der Download seite sehr wichtig, sobald man einen Link zu einer Webseite aufruft, sollte die URL auf korrektheit korrigiert werden, wenn die URL nicht durch einen HTTPS angeführt wird, sollte man die Webseite schnellstens verlassen.

→ Kinderschutzfilter
Überwachung von Browser- und E-Mail-Aktivitäten auf Schadprogramme
erweiterte, verhaltensbasierte Erkennung von Schadsoftware

Schadprogramme / Malware

Arten: Virus, Wurm, Trojaner, Backdoor, Spyware, Scareware, Ransomware, Grayware, Rogueware

Wie kann man sich schützen?

- Noch nie genutzte Programme erst einmal in einer Sandbox installieren und ausprobieren
- Virenschutz installieren
- Keine Zwielichtigen Installer Ausführen
- Nur seriöse Webseiten zum Download von Programmen nutzen
- Beim Installer aufpassen das keine Adware mitinstalliert wird.

Welches Schädigungspotential gibt es?

- Kompletter Datenverlust
- Identitätsdiebstahl
- Kontozugriff (Bankkonto etc.)

Infektionswege:

→ E-Mail
→ Externe Datenträger
→ Smartphone
→ Smart Home

E-Mail:
→ Keine Anhänge von nicht vertrauenswürdigen E-Mails öffnen
→ nicht auf Links in Mails / Werbebanner klicken

USB-Stick:
→ keine werbe-sticks verwenden
→ Keine Installations Sticks verwenden, wegen zusatz softwares

Smartphone:
→ Apps aus den App-stores laden
→ keine drittanbieter Software verwenden
→ Bowser bewusst verwenden / keine werbebanner anklicken

Smart Home
→ Mehr fokus auf sicherheit legen
→ Augenmerk auf guten Support
→ Router ständig aktuell halten

Spam, Phising & Co.

Formen unerwünschter Post:
- Brief, Telefonat, E-Mail, Fax, Apps

Erkennungsmerkmale:
- Absender
- Hyperlinks
- Rechtschreibung
- Fehlender Name
- Aufforderung zum öffnen einer Datei
- Nicht Kunde oder erste E-Mail erhalten von Banken

Schutzmaßnahmen:
- manuelle Eingabe von Internetseiten
- Anrufe ignorieren, oder eingaben von Kontonummer, Tan oder Pin
- Virenschutz Software und Firewall Einschalten
- System Aktuell halten

Erkennungsmerkmale für falsche Absenderadressen und Schutzmaßnahmen
- Fremde E-Mail-Adresse
- Fehlender Kundenname
- Aufforderungen z.B. Telefonnummer anrufen, E-Mail beantworten, persönliche Daten preisgeben
- Gefährliche Datei anhänge

Jannik Singer, Tobias Arras, Dante Neumann, Florian Hinkelmann