Malware in Unternehmen: Verbreitung und Massnahmen

Hochschule Luzern, Campus Zug-Rotkreuz, Rotkreuz

Christian Birchler, Stephan Verbücheln
21. November 2019

cnlab

Agenda

- Moderne Malware
- Infektion, Verbreitung und Wirkung
- Schutzmassnahmen

Typen von Malware (die wichtigsten)

- Viren
  - Malware, die sich verbreitet und versteckt, indem sie andere Programme «verseucht».
- Dropper
  - Malware, die andere Malware nachlädt.
- Würmer
  - Malware, die sich selbst ohne Zutun des Benutzers verbreitet.
- Trojaner
  - Malware, die sich verdeckt hält und spioniert, ggf. andere Funktionen nachlädt.
- Ransomware
  - Malware, die das Opfer erpresst.
  - Meist, indem sie Daten verschlüsselt.

Aktuelle Malware (Auswahl)

- Emotet
  - ursprünglich Banking-Trojaner, Ziel deutschsprachiger Raum
  - mittlerweile Vehikel für andere Malware (Dropper)
- Trickbot
  - Banking-Trojaner
  - stiehlt Login-Daten, Kartennummern, TANs usw.
- Ryuk
  - Ransomware
  - verschlüsselt Daten und erpresst Opfer

Verbreitungswege: Infektion

- E-Mail
  - Benutzer werden dazu gebracht, bösartige Dateien zu öffnen
    - E-Mail-Anhänge
    - Links
- Unsichere Konfiguration
  - Unnötige Funktionen sind erlaubt
    - Office-Makros, USB-Sticks
- Sicherheitslücken
  - Lokales System (Windows-Rechner)
  - Unsichere Anwendungen (Browser, E-Mail, Office)
- Supply Chain
  - Geräte oder Software schon beim Hersteller infiziert

Verbreitungswege: Interne Weiterverbreitung

- E-Mail
  - Malware benutzt Adressbücher und E-Mails zur Weiterverbreitung
- Unsichere Konfiguration
  - Malware versucht sich über zentrale Infrastruktur zu verteilen (Fileserver, Anwendungen)
  - Malware stiehlt Benutzername/Passwort (Active Directory)
    - Keylogger, Phishing
- Sicherheitslücken
  - Internes Netzwerk (häufig SMB-Schwachstellen)
  - Lokales System (Windows-Rechner)
  - Unsichere Anwendungen (Browser, E-Mail, Office)

Wie gehen Angreifer vor?

- Informationen sammeln
  - Adressbücher, Active Directory
  - Lokale Server
  - Gibt es interessante Daten?
  - Wie hoch ist der Wert im Falle einer Erpressung?
- Daten ausspionieren
  - Zahlungsdaten (Bankdaten, Kreditkartendaten, usw.)
  - Credentials für weitere Systeme
  - Betriebsgeheimnisse
- Lokal Schaden anrichten
  - Verschlüsselung von Daten, Löschen von Backups
  - Kommunikation zum Opfer (Erpressung)

Umgang mit Vorfällen

- Je früher ein Vorfall entdeckt wird, desto besser kann man darauf reagieren

- Problem: Mitarbeiter melden Vorfälle nicht, da sie negative Konsequenzen fürchten
  - Gute Kommunikation mit den Mitarbeitern

- Dasselbe gilt für Unternehmen gegenüber Geschäftspartnern und Kunden
  - Häufig sind vertragliche und regulatorische Verpflichtungen zu beachten

Risiken

Traditionell

- Betriebsausfälle
- Unerwünschte Zahlungen

Aktuell

- Reputation
- Erpressung

Durch die richtigen Massnahmen können Eintrittswahrscheinlichkeit reduziert und Schaden begrenzt werden.

Massnahmen

- Verhältnismässig wählen
- Konsequent durchsetzen
- Verifizieren

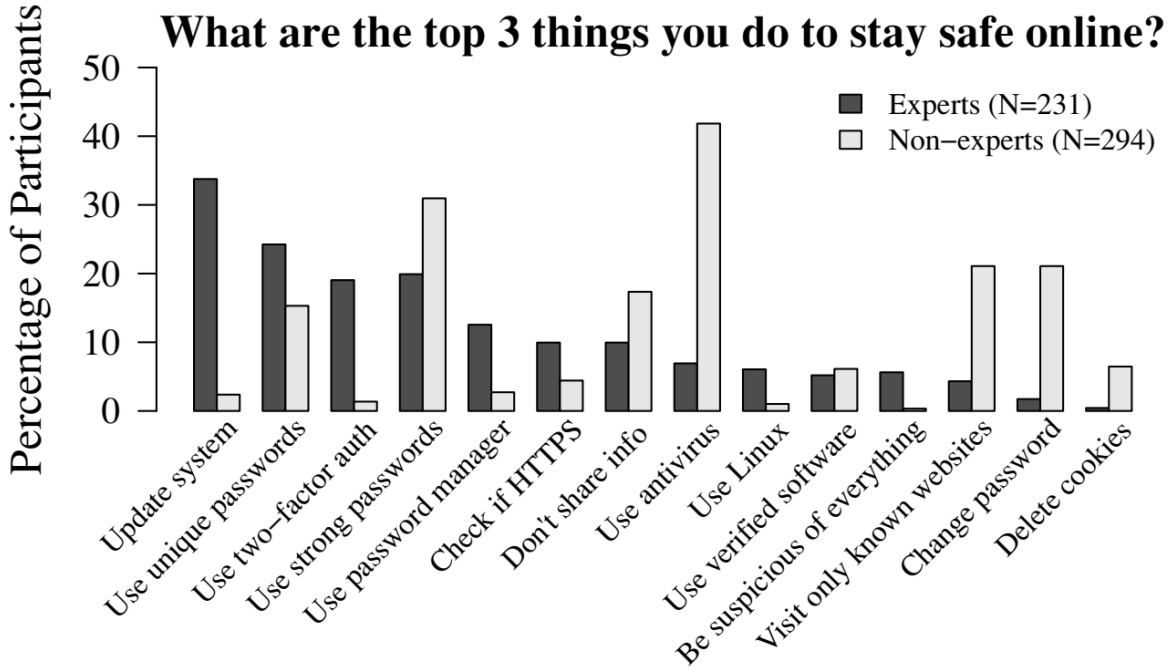


Figure 1: Security measures mentioned by at least 5% of each group. While most experts said they keep their system updated and use two-factor authentication to stay safe online, non-experts emphasized using antivirus software and using strong passwords.

Quelle: Google Umfrage «"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices», Symposium on Usable Privacy and Security

Massnahme: Backup

Schadensbegrenzung

IT-Standard

- Verfügbarkeit der Daten und Systeme im Fall von technischen Problemen
  - Ausfall eines Servers
  - Ausfall von Festplatten
- Grundregel: Eine Sicherheitskopie ist nur dann ein Backup, wenn es wiederhergestellt werden kann.

Malware (zusätzlich)

- Unveränderbarkeit der Daten und Systeme
  - Erpressung ist wirkungslos, wenn das Opfer eine intakte Kopie hat
- Grundregel: Eine Sicherheitskopie ist nur nützlich, wenn sie vom Angreifer nicht verändert werden kann.

Massnahme: Update-Management

Schutz gegen Infektion

IT-Standard

- Viele Programme verarbeiten Daten unbekannten Ursprungs
  - Anhänge von E-Mails (Kunden, Geschäftspartner)
  - Downloads aus dem Internet

Malware

- Diese Programme müssen immer aktuell gehalten werden
  - Betriebssystem
  - Browser, E-Mail, Messenger
  - Office-Suite, PDF-Reader, Tools generell

Massnahme: Awareness-Schulung

Schutz gegen Infektion

IT-Standard

- Sensibilisierung der Mitarbeiter

Malware (zusätzlich)

- Hohe Sensibilisierung notwendig, Phishing-Angriffe können vom internen Netzwerk kommen

Massnahme: Filtern

Schutz gegen Infektion

IT-Standard

- E-Mail (Filter auf Malware und Phishing)
- Internet-Zugang (Filter auf Malware und Phishing)
- Restriktive Zugriffsberechtigungen auf Files
- File-Server (Scan auf Schadcode)

Malware (zusätzlich)

- Aktive Auswertung von Protokolldaten
- Webisolation

Massnahme: Berechtigungen

Schutz gegen Verbreitung

IT-Standard

- Mitarbeiter haben Zugriff (lesend und scheibend) auf Daten, die sie nicht benötigen
- Mitarbeiter haben administrative Berechtigung an ihrem Arbeitsgerät
- Administratoren benutzen ihr Arbeitskennwort auch zur Systemverwaltung (Active Directory)

Massnahme

- Rigorose Einschränkung der Zugriffsberechtigungen
- Keine administrativen Berechtigungen für Benutzer

Schwierigkeiten

- Berechtigungskonzept: Starke Einschränkungen behindern die Arbeit

Massnahme: Netzwerk, Zonierung

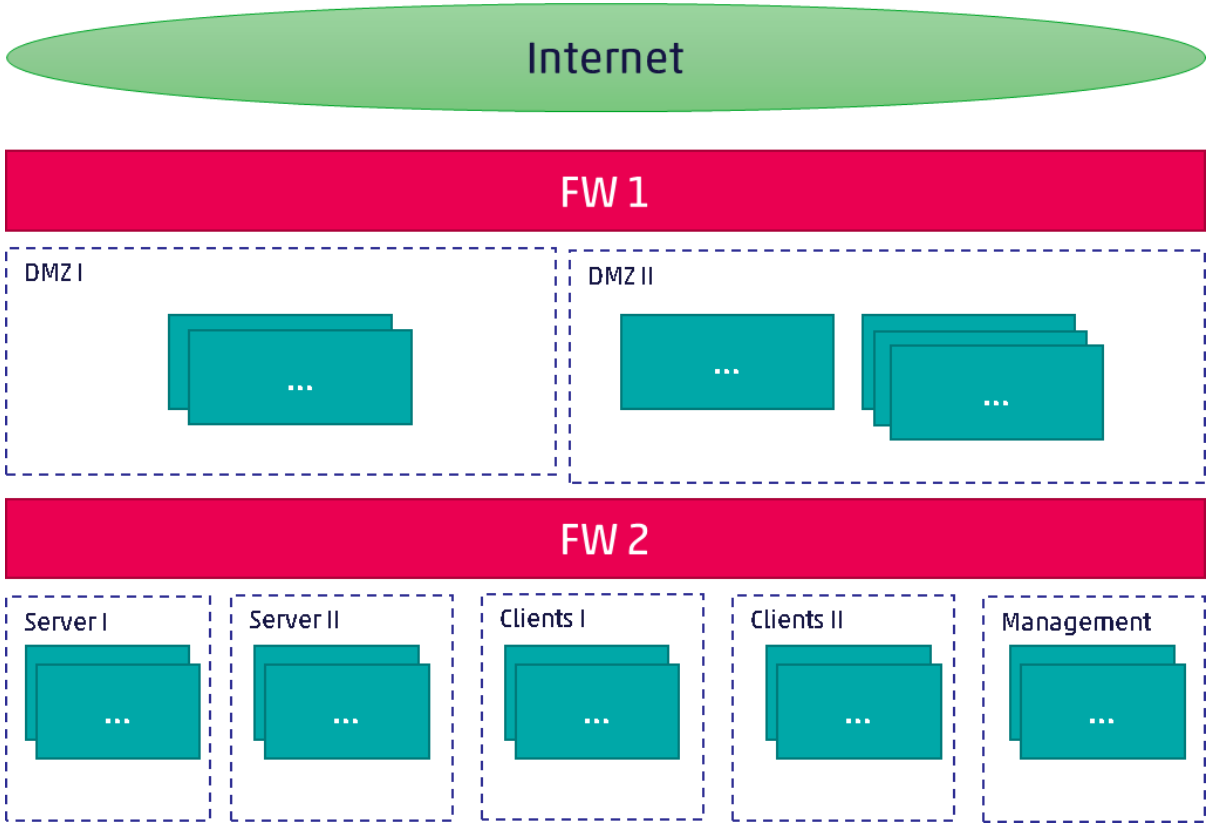
Schutz gegen Verbreitung

IT-Standard

- Flache Strukturen oder einfache Zonierung (Perimeter-Schutz)

Malware

- Zonierung behindert Ausbreitung
  - Interaktion zwischen Clients verhindern
  - Server-zu-Server-Kommunikation einschränken
  - Dediziertes Management-Netz
- Abtrennung der Backup-Systeme



Massnahme: Protokollierung und Monitoring

Schutz gegen Verbreitung

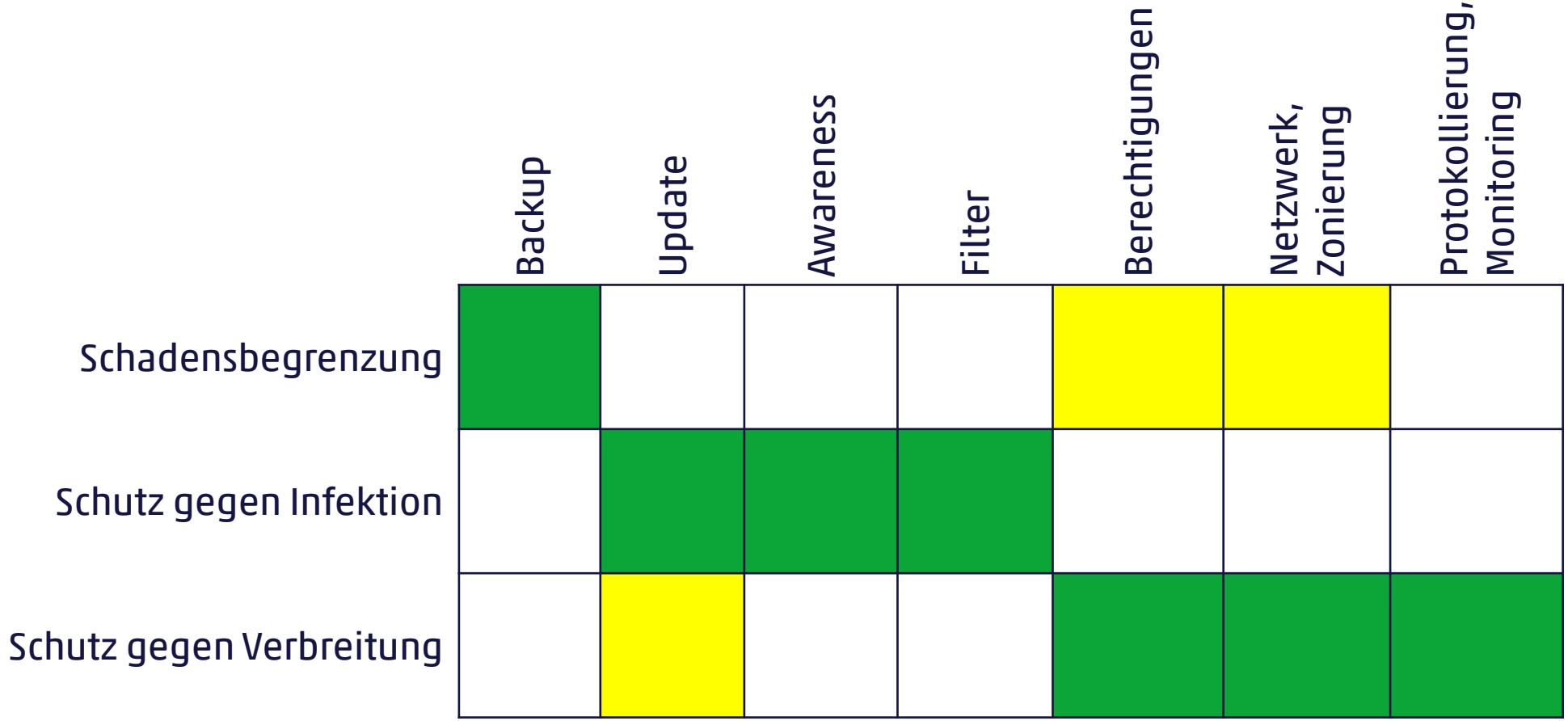
IT-Standard

- Nachvollzug von Benutzer-Aktivitäten und System-Verhalten

Malware

- Analyse im Rahmen des Incident-Managements (Nachforschungen)

Positionierung der Massnahmen



Behebung

- Sofortmassnahmen (Schadensbegrenzung)
  - Alle Systeme im betroffenen Segment (Netzwerkzone, Active-Directory-Domain) ausschalten/trennen,
  - Alternative Arbeitsumgebung aufbauen oder aktivieren.

- Mittelfristige Massnahmen (Schaden beheben)
  - Einsatz einer Task-Force (Notfallorganisation)
  - Information an Kunden und Partner,
  - Forensische Untersuchung der Infektion,
  - Aufbau einer intakten Umgebung,
  - Wiederherstellung der Daten (ab Backup),
  - Nacharbeiten.

- Längerfristige Massnahmen (zukünftige Schäden verhindern)

Prüfung der Massnahmen

Warum braucht es eine Prüfung?

- Die Massnahmen sind im regulären Betrieb nicht sichtbar (z.B. Zonierung)
- Aufweichung der Massnahmen, da diese hinderlich sind
- Prüfungen gegen Standards reichen nicht (zu wenig spezifisch)

Fazit

- Die Wahrscheinlichkeit einer Infektion ist heute hoch. Gute Massnahmen machen das Risiko beherrschbar.
- Alte Massnahmen sind nicht wirkungslos geworden, Angreifer passen sich jedoch an.
- Massnahmen müssen professionell organisiert werden.
- Gute Massnahmen sind aufwendig und müssen langfristig ausgelegt sein.
- Ein Befall stellt einen Notfall dar für viele Unternehmen. Man muss entsprechend reagieren.

Lektüreempfehlungen zum Thema

Bericht des **Heise-Verlags** über Emotet und Co.

https://www.heise.de/security/artikel/...4573848.html

Halbjahresbericht von **MELANI** über Cyberangriffe in der Schweiz und international 2019/1 mit **Schwerpunkt Verschlüsselungsmalware**

https://www.melani.admin.ch/melani/de/.../halbjahresbericht-2019-1.html

Vielen Dank für Ihre Aufmerksamkeit_

Christian Birchler
+41 55 214 33 40

Stephan Verbücheln
+41 55 214 33 36

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab Speedtest

https://speedtest.cnlab.ch

Datenschutzkurs

https://datenschutzkurs.ch

cnlab