cubewerk

· weil uns IT begeistert ·

cubewerk GmbH
Herzog-Otto-Str. 32
83308 Trostberg
08621-9883088

support@cubewerk.de
www.cubewerk.de

Best-Practice Tasks

Abwehr/Erkennung von Emotet/Crypto-Trojanern in Microsoft-Netzwerken

Stand: 09.09.2019
Autor: Stefan Bauer
Grad: public

cubewerk

· weil uns IT begeistert ·

Vorwort:

Angriffe auf IT-Systeme nehmen drastisch zu. Das BSI bündelt seit 2012 Kompetenzen in der Allianz für Cybersicherheit, welcher auch die cubewerk GmbH angehört.

Nachfolgende Maßnahmen bieten Empfehlungen für KMUs zur Absicherung der IT-Umgebungen gegen Cyberangriffe und Verschlüsselungstrojaner.

Die Maßnahmen stellen TOMs (technische und organisatorische Maßnahmen) dar, die seit Einführung der DSGVO auch rechtlich konkret gefordert sind (Art. 32 DSGVO).

Technische Maßnahmen:

Maßnahme
Perimeter-Firewall / Netztrennung (VLANs, Subnetze, Zonenkonzept)
AntiSpam- und AntiVirus-Lösungen – so weit wie möglich außerhalb der Firma. Mögliche Einfallstore wie E-Mail, Dateiaustausch, Web-Download sollten so weit wie möglich, von der internen IT getrennt sein und möglichst weit außerhalb gefiltert werden. Z. B. Externe Cloudlösung für AntiSpam- und AntiVirus, definierte Wege, wie Daten in Firma kommen dürfen.
Definition, dass z. B. interne E-Mails (von eigener Domain) niemals von außen kommen dürfen. Möglich u.U. durch Definition auf AntiSpam-Appliance/Filter
Command & Control-Server in AntiSpam-Lösungen aktuell halten/filtern und zusätzlich in Firewalls blocken & aktualisieren und durch angepasstes Monitoring auch überwachen (https://paste.cryptolaemus.com/)
Abuse.CH Ransomware Tracker verwenden als zusätzliche Blacklist für C&C-Tracker (https://ransomwaretracker.abuse.ch/blocklist/) sowie FedoTracker (https://feodotracker.abuse.ch/blocklist/)
Aktuelle lokale Endpoint-Protection (Virenschutz) inkl. Überwachung, ob diese aktuell ist und auch läuft
Forcierte Update-Richtlinien für Clients, Benutzern keine Wahl lassen zur Installation (Windows-Updates z. B.)
Abgesicherte Software nutzen, wo es möglich ist. Z.B. kann ein Office-PC auch mit Linux und Open/Libre-Office betrieben werden im Unternehmen
Microsoft-Office-Macros via GPOs blockieren oder gleich durch Mailfilter Anhänge blockieren
Powershell Constraint Language Mode deaktivieren via GPO
Verbieten von Kennwortspeicherung im Browser
Windows-Client Sicherheitsfunktionen erzwingen (Guard, Defender) und diese Zustände auch automatisiert überwachen (z. B. Um Probleme nach automatisierten Windows-Updates zu erkennen)
Netzwerkaktivitäten überwachen durch Honeypots (dedizierter PC/Client im Haus, der keine Funktion hat aber Dienste bereitstellt um auffällige Anmeldungen oder Aktionen frühzeitig zu erkennen)
Zentraler Logserver im Haus, welcher sämtliche Log-Dateien von Systemen einsammelt und unlöschbar vorhält (z. B. Kibana / Logstash-System auf dediziertem Linux-Loghost) ohne Domänenmitgliedschaft.

Kennwort-Richtlinie erzwingen sowie Rotierung von Kennwörtern erzwingen (mind. 32-Zeichen Kennwörter, alle 12 Monate wechseln).
Getrennte Systeme/Hardware für Adminaufgaben mit optionaler 2FA (zweiter Faktor).
Getrennte Benutzerkonten für Benutzer/Admin (selbe Person besitzt zwei Accounts)
Lokale Administratoren verbieten an PCs
Datensicherung auslagern. Eine Datensicherung darf nicht durch einen Admin gelöscht werden können. Notfalls auf read-only-System wegkopieren (es muss nicht immer teures WORM-System sein). Es reicht oft physikalische Trennung/Abschottung.

Organisatorische Maßnahmen:

Maßnahme
IT-Awareness / Mitarbeiterschulungen im Umgang mit Viren/Trojanern/Auffälligkeiten im Umgang mit IT-Systemen inkl. Regelmäßiger Auffrischung
Ausnahmen in der Behandlung von einzelnen Mitarbeitern vermeiden (keine Sonderlocken für CEO, Praktikanten oder Buchhaltung bzw. Entwickler)
Firmenweite Policy aufstellen/formulieren, welche Anwendungen / Endungen / Tools erlaubt sind und welche explizit verboten.
Allen Benutzern Administrationsrechte entziehen, die diese nicht zwingend benötigen – nicht nur domänenweit sondern auch auf lokalen Arbeitsplätzen
Regelmäßige IT-Stichproben / IT-Begehung inkl. Dokumentierung im Unternehmen (monatlich). Keine Verharmlosung von Vorfällen
Definieren, wie Anwendungen im Haus genutzt werden dürfen und wer welche Anwendungen frei gibt, Vermeidung von Download-und-Start-Anwendungen, Richtlinien formulieren
Regelmäßige Deaktivierung von Benutzern / Ablaufdatum von Accounts festlegen
Bewusst Software auswählen, Inventur von eingesetzter Software, u.U. nicht mehr gewartete Software im Einsatz ausmisten
Definition, wer macht Updates von Anwendersoftware auf Arbeitsplätzen in welchem Intervall
Definition / Rechte von Service-Accounts prüfen – spezielle auch jeden mit Kerberos-TGT-Keytab-Dateien für SSO
IT-Sicherheitsablauf besprechen, was wäre wenn?
Interne Planspiele – was wäre wenn, Maßnahme X nicht greift, doppelter Boden vorhanden?
Assets definieren, mit welchen Daten wäre die Firma nicht arbeitsfähig. Diesen Assets höhere Priorität zuteilen und daran Maßnahmen festmachen

Fazit:

IT-Sicherheit ist ein dauerhafter Prozess. Bei der Auswahl von Software sollte bewusst auf OpenSource-Software gesetzt werden. Eingesetzte Lösungen müssen regelmäßig neu bewertet werden.