Schadsoftware

Problembeschreibung und Ursache

Schadsoftware ist nicht nur für die IT ein weit verbreitetes Problem, sondern auch in der OT gab es bereits mehrere Fälle von Angriffen mittels Schadsoftware. Zu den bekanntesten OT-Sicherheitsvorfällen zählen u.a. Stuxnet oder CrashOverride. Die Malware CrashOverride z.B. war auf Stromnetze ausgelegt, welche Stromausfälle in der Ukraine verursachten.

Schadsoftware kann über mehrere Wege eingeschleust werden, wie z.B. über Schwachstellen von IT-/OT-Komponenten oder durch Platzierung von infizierten Wechseldatenträgern im Intranet. Die Sicherheit gegen Schadsoftware wird durch die zunehmnde Verbreitung ethernet-basierter Netze und Protokolle im ICS-Umfeld und deren Verbindung mit Systemen im Unternehmensnetz erschwert. Wie bereits im Level Netzwerksegmentierung behandelt wurde, kann ein Angreifer, der in das Office-Netz vorgedrungen ist, bei schwacher Netzwerksegmentierung einen Folgeangriff auf das OT-Netz ausüben.

Bedrohungsszenarien

Die wohl größte und gefährlichste Bedrohung in Bezug auf Schadsoftware sind die sogenannten Zero-Day-Exploits. Zero-Days sind Schwachstellen in Systemen und Software, von denen nur Hacker wissen. Das bedeutet, dass es dafür keine Patches gibt und es bietet einen Weg zur Einschleusung von Schadsoftware.

Doch es gibt auch andere Wege, mit denen Schadsoftware eingeschleust werden kann. Beispielsweise bietet die Installation von private Hardware, wie z.B. Spielkonsolen oder eines eigenen WLAN-Routers im Unternehmen einen weiteren Angriffspfad für Hacker, da diese Hardware außerhalb vom Unternehmensnetz bzw. vor der Installation im Unternehmensnetz infiziert werden könnte. Eine weitere Gefahr besteht darin, dass die Webseite des Unternehmens angegriffen werden kann. Ist diese nicht ausreichend abgesichert, kann sich ein Hacker möglicherweise Zugang zum Webserver verschaffen, wodurch er weiter in das IT-Netz vordringen kann. Sind dann die Maßnahmen aus Level 1 (Netzwerksegmentierung) nicht umgesetzt, kann der Hacker einen Folgeangriff auf das OT-Netz ausführen.

Gegenmaßnahmen und Sicherheitsvorkehrungen

Im Folgenden wird aufgelistet, welche Maßnahmen man ergreifen sollte, um sich so gut wie möglich gegen Schadsoftware zu schützen.

Allgemeine Gegenmaßnahmen

- Durchsetzung der Maßnahmen für die Netzwerksegmentierung
- Ungeschützte bzw. unpatchbare Systeme sollten abgeschottet werden

- Schutzmaßnahmen wie Antivirenschutz, Firewall, Whitelisting, Überprüfung digitaler Signaturen
- Die im Unternehmen frei verfügbaren Informationen auf ein Minimum zu beschränken, um kritische Informationen zu schützen (principle of least privilege)
- Regelmäßiges und zeitnahes Patchen von Betriebssystemen, Office-Anwendungen usw. und wo möglich im ICS-Netz
- Monitoring von Logfiles auf ungewöhnliche Verbindungen/Verbindungsversuche
- Härtung von IT-Komponenten im Office- sowie ICS-Netz

Überprüfung auf Schadsoftware

Alle Geräte und mobilen Datenträger müssen vor der Nutzung auf Schadsoftware überprüft werden. Die Gefahr hierbei besteht darin, dass Geräte bzw. mobile Datenträger vor oder während des Transports infiziert werden können. Bei verschlüsselten Datenträgern soll ebenfalls eine Überprüfung möglich sein. Die Überprüfung auf Schadsoftware kann auf zwei Arten erfolgen:

- Authentizitätsprüfung: kann z.B. durch digitale Signaturen festellen, ob Software-Abbilder im Gerät nicht verändert wurden
- Scannen: falls Authentizitätsprüfung nicht unterstützt wird: Scannen von bekannter Schadsoftware

Schutz gegen Schadsoftware

Es muss auf allen Geräten eine Software zum Schutz gegen Schadsoftware installiert sein. Leider ist oft nicht für alle ICS-Geräte eine solche Software verfügbar. Diese Geräte sollten dokumentiert werden und es müssen Ausgleichsmaßnahmen zum Schutz dieser Geräte umgesetzt werden. Es gibt drei primäre Methoden zum Schutz gegen Schadsoftware:

- Virenschutz: wird verwendet, um Dateien und Daten, die auf das Gerät gelangen, mit der Signatur (bekannte Bit-Muster) zu vergleichen (Blacklisting), und bei Feststellung von Schadsoftware wird diese unter Quarantäne gestellt und der Benutzer wird benachrichtigt
- Whitelisting: nur autorisierte Software kann ausgeführt werden
- Überprüfung digitaler Signaturen: Authentifizierung von Hashes von Software (Form von Whitelisting)

Die Software zum Schutz gegen Schadsoftware sollte zeitnah nach ihrer Freigabe installiert werden, da das ICS in dieser Zeit anfällig ist.

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente SPE4 - Komponentensicherheit: COMP2 - Schutz vor Schadsoftware, und einem Dokument des BSI über Top 10 Bedrohungen und Gegenmaßnahmen für ICS: Infektion mit Schadsoftware über Internet und Intranet (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1)