Zweischneidig

Volker Oestreich

Messenger, Wetterprognosen, Navigationssysteme, Spiele: Wie viele dieser Anwendungen haben Sie auf Ihr Smartphone geladen? Millionen von vermeintlich kostenlosen Apps werden zum Download angeboten, doch wir zahlen mit unseren persönlichen Daten und Nutzungsgewohnheiten: Aufenthaltsort, Kommunikation, Einkäufe, Vorlieben bei Filmen und Musik, alles wird von App-Anbietern aufgezeichnet. Forscher u.a. des Karlsruher Instituts für Technologie (KIT) haben nun eine Datenschutz-App entwickelt, welche die eigenen Daten besser schützen soll, aber trotzdem die uneingeschränkte Nutzung beliebter aber informationshungriger Anwendungen erlaubt.

Das Programm Avare (www.avare.app) lässt sich auf Android-Geräten wie eine App installieren und erzeugt dann einen abgeschlossenen Bereich, in den andere Apps eingepackt werden können und der die gesamte Kommunikation zwischen diesen Apps und dem Betriebssystem kontrolliert. Dabei haben die Entwickler einen Weg gesucht, der es erlaubt, sämtliche Anwendungen uneingeschränkt zu nutzen, dabei die eigenen Daten aber nur kontrolliert weiterzugeben.

Das hört sich gut an, ist aber eine zweischneidige Geschichte. Hinter der Entwicklung all der vielen geliebten und oft auch nützlichen „kostenlosen" Apps stehen Geschäftsmodelle, bei denen die Entwicklungskosten, oft mit sehr hoher Rendite, über das spätere Handeln mit gewonnen Daten eingespielt werden. Versiegt diese Quelle, müssen neue Geschäftsmodelle gefunden werden oder es gibt keine neuen kostenlosen Apps mehr. Da ergeben sich spannende Herausforderungen für beide Seiten, Datenkraken und Datenschützer.

Zweischneidig ist auch die immer intensivere Vernetzung von unternehmenskritischen OT- und IT-Netzwerken im Rahmen von IIoT und Industrie 4.0. Den enormen sich bietenden Vorteilen stehen neue, oft schwer kalkulierbare Risiken gegenüber. Eines ist die Gefahr durch Ransom-Software: Nach Drogenhandel und Schutzgelderpressung hat die mehr oder weniger organisierte Kriminalität ein neues Geschäftsmodell aufgetan mit dem Vorteil, weltweit und gut geschützt agieren zu können.

Ich wünsche Ihnen, wie immer, ein gutes und erfolgreiches Studium Ihres aktuellen CHEManager – in dieser Ausgabe mit Vorschlägen, wie die neuen Herausforderungen für die Cyber-Sicherheit in OT-Netzwerken zu meistern sind. Wir bieten Ihnen heute und in Zukunft die Informationen, die Ihnen helfen, nachhaltig die Belange Ihres Unternehmens, Ihrer Mitarbeiter und Ihrer Umwelt zu verfolgen.

Ihr

voe@voe-consulting.de

Monitoring und Anomalieerkennung

Cyber-Angriffe auf Industrienetzwerke nehmen zu

Mit der zu beobachtenden Zunahme von Angriffen auf Produktionsnetzwerke und Netze in kritischen Infrastrukturen werden Maßnahmen zur Erkennung solcher Angriffe mehr denn je erforderlich. Diese müssen den komplexen Strukturen gerecht werden und erfordern daher entsprechende Systeme. Monitoring und Anomalieerkennung sind wichtige Komponenten der Verteidigungsstrategie.

Monitoring macht die Teilnehmer und Kommunikationsbeziehungen in einem Produktionsnetzwerk transparent und dient damit den allgemeinen Zwecken der Inbetriebnahme und Wartung. Als Überwachungslösung ist Monitoring ein geeignetes Mittel, um Abweichungen von vorgegebenen Verhaltensweisen und festgelegten Mustern zu erkennen. Anomalieerkennung ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze. Dies unterscheidet die Anomalieerkennung von anderen Maßnahmen, die auf der Erkennung bereits bekannter Angriffe beruhen. In einer kürzlich veröffentlichten Cyber-Sicherheits-Empfehlung weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf die Bedeutung von „Monitoring und Anomalieerkennung in Produktionsnetzwerken" hin.

Nur wenn wir IT Security als Voraussetzung der Digitalisierung begreifen, können wir langfristig von ihr profitieren.

Arne Schönbohm, BSI-Präsident

Anomalien in prozesstechnischen Anlagen

Normungen und Vorgaben erfüllen das Herz eines Betreibers nicht immer mit Freude. Bei der BSI CS 134 wurde allerdings ein wichtiger Schritt in die richtige Richtung der IT / OT Security gemacht. Davon ist Dieter Barelmann, CEO von Videc Data Engineering, überzeugt. Er beschreibt den Ist-Zustand vieler Anlagen bezüglich der Security-Maßnahmen so: „Man stelle sich einmal vor, wir würden heute in prozesstechnischen Anlagen ohne Leit- oder SCADA System Produkte herstellen wollen. Keine Sichtbarkeit, keine Kontrolle über den Prozess. Die Automatisierung läuft, jedoch kann man nichts über den Zustand der Anlage aussagen. Undenkbar – aber im Bereich der OT Security ist es Stand der Dinge."

Durch die immense Erhöhung der Teilnehmer in Prozessanlagen und entsprechend auch der Kommunikation ist kaum noch jemandem bekannt, wer mit wem kommuniziert – berechtigt oder auch nicht; insbesondere wenn mehrere Anlagenteile von unterschiedlichen Lieferanten installiert werden. „Durch die steigende Komplexität im Netzwerk und die Implementierung von nicht immer vollständig IP-standardkonformen Geräten kommt es immer wieder zu Seiteneffekten im Netzwerk, die zunächst nicht bemerkt werden und irgendwann zu einem Störfall werden können. Dies wäre mit einer kontinuierlichen Überwachung des Netzwerkverkehrs aufgefallen und vermeidbar gewesen", äußert sich Barelmann und bricht eine Lanze für das passive Monitoring: „Wenn erst einmal ein Netzwerk z.B. über einen infizierten Programmierrechner unbemerkt befallen ist, kann sich der Angreifer weiter austoben. Sogar Schadcode nachzuladen würde von einer Firewall nicht verhindert werden, da der Verbindungsaufbau ins Internet aus der internen Zone erfolgt. Hier hat das BSI aus Sicht der IT-Sicherheit dem Hase-und-Igel-Spiel zwischen dem Angreifer und dem Schützenden einen wichtigen Impuls zugunsten des Betreibers gegeben. Die Vorteile des passiven Monitorings sind dabei neben der Möglichkeit der Angriffserkennung vielschichtig: Jeder Anlagenbetreiber hat sofort alle Teilnehmer im Blick und externe Dienstleister lassen sich über die Zugänge genau kontrollieren. Zusätzlich erhält die IT wichtige Informationen für die Feinjustierung der Firewall, ein wichtiger Punkt bei der Angriffsabwehr. Bei der Alarmierung in der Angriffserkennung lässt sich der Servicebereich in der Regel optimieren und spart Kosten."

Die unterschiedlichen Ansichten über eine aktive bzw. passive Abfrage der Assets sind für Barelmann aus Sicht der Automatisierung sehr einfach zu klären: Die sensible Struktur der Automatisierungsgeräte mit ihren unterschiedlichen Generationen ist bei einem 24/7 Betrieb keine Spielwiese für aktive Abfragen. Das höchste Gut der OT ist die Verfügbarkeit – diese verträgt lediglich die passive Variante.

Gezielte Cyber-Angriffe auf Unternehmen

Generell registriert das BSI derzeit verstärkt Netzwerkkompromittierungen bei Unternehmen, die mit der manuellen und gezielten Ausführung eines Verschlüsselungstrojaners (Ransomware) enden. Dabei verschaffen sich die Angreifer mittels breit angelegter Spam-Kampagnen wie Emotet zunächst Zugang zu einzelnen Unternehmensnetzwerken und erforschen dann manuell Netzwerk und Systeme der Betroffenen. "Wir erleben derzeit die massenhafte Verbreitung von raffinierten Angriffsmethoden durch die organisierte Kriminalität, die bis vor einigen Monaten nachrichtendienstlichen Akteuren vorbehalten waren. Unternehmen sollten auch kleine IT-Sicherheitsvorfälle ernst nehmen und ihnen konsequent begegnen, da es sich dabei durchaus auch um vorbereitende Angriffe handeln kann", konstatiert BSI-Präsident Arne Schönbohm.

Wir beobachten einen Anstieg der Angriffe auf deutsche Unternehmen mit teilweise existenzbedrohenden Datenverlusten.

Jens Wiesner, BSI

Das BSI konnte in den letzten Monaten großangelegte Malware-Kampagnen analysieren, bei denen vor allem maliziöse Anhänge oder Links zu gefälschten Webseiten in massenhaft versendeten Spam-Mails als Einfallsvektor dienten. Nach einer erfolgreichen Infektion wurde häufig weitere Malware (z.B. Trickbot) nachgeladen, um sich im Netzwerk auszubreiten, Zugangsdaten zu erbeuten und das Netzwerk bzw. die Systeme auszuwerten. Nach einer erfolgreichen Ransomware-Infektion sind teilweise sehr hohe Bitcoin-Forderungen gestellt worden. Dabei sind wiederholt keine pauschalen Forderungen aufgestellt, sondern individuelle Zahlungen ausgehandelt worden.

Insbesondere in Deutschland ist diese Vorgehensweise verstärkt mit der Ransomware GandCrab beobachtet worden. Bei den bekannten Fällen haben die Angreifer sich zunächst über Fernwartungstools (z.B. RDP, RescueAssist, LogMeIn) Zugriff auf das Netzwerk verschafft, auf verschiedenen Systemen im Netzwerk der Opfer eine Backdoor installiert, potentielle weitere Opfer ausgespäht und schließlich die Ransomware zur Ausführung gebracht.

Obwohl bei diesem Szenario prinzipiell keine neuartigen Angriffstechniken verwendet werden, waren derartig gezielte und manuell ausgeführte Angriffe im Cybercrime-Umfeld bisher selten zu beobachten. Insbesondere die folgenden drei Aspekte sind zu berücksichtigen:

- Jede einfache Infektion kann zu einem gezielten Angriff führen, da die Angreifer sich zunächst über groß angelegte Kampagnen Zugriff auf viele Netzwerke verschaffen. Jede Primärinfektion (z.B. mit Emotet) kann später weitreichende Folgen haben. Es sollte genau geprüft werden, welche Zugangsdaten potenziell abgeflossen sein könnten und Maßnahmen ergriffen werden, die eine spätere Rückkehr des Angreifers verhindern.
- Es droht ein kompletter Datenverlust, da im Gegensatz zu automatisierten und breit angelegten Ransomware-Kampagnen die manuell ausgeführten Angriffe zwar einen deutlich höheren Arbeitsaufwand für die Angreifer bedeuten, sie jedoch gezielt lukrativere Ziele angreifen und u.U. Backups so manipulieren bzw. löschen, dass diese nicht mehr zur Wiederherstellung der Systeme zur Verfügung stehen.
- Die Gefahr für deutsche Unternehmen steigt. Das BSI beobachtet einen Anstieg der Fallzahlen bei deutschen Unternehmen mit teilweise existenzbedrohenden Datenverlusten. Dabei haben unterschiedliche Gruppen unterschiedliche Ransomware und Tools verwendet.

Unternehmen, die eine Malware-Infektion erlitten haben, sollten Geschäftspartner oder Kunden zeitnah über den Vorfall informieren und auf mögliche zukünftige Angriffsversuche per E-Mail mit gefälschten Absenderadressen ihrer Organisation hinweisen.

Um sicherzugehen, dass die Unternehmen nicht selbst durch einen Geschäftspartner oder Dienstleister infiziert werden, sollten Netzwerkzugriffe und die Berechtigungen externer Dienstleister überprüft werden. Sollte der Dienstleister selbst Opfer eines Ransomware-Angriffs werden, könnten die Angreifer sonst z.B. über existierende VPN-Verbindungen in das eigene Firmennetzwerk eindringen.

Keine Sichtbarkeit, keine Kontrolle über den Datenverkehr – im Bereich der OT Security ist es Stand der Dinge.

Dieter Barelmann, Videc Data Engineering

Grundsätzlich rät das BSI dringend davon ab, auf etwaige Forderungen der Täter einzugehen.

Angriffspfade und Fehlerkultur

Auch auf die Prozessindustrie sind in jüngster Zeit zahlreiche dokumentierte Angriffe ausgeübt worden. Darauf weist Jens Wiesner, Referatsleiter „Cybersicherheit in Industrieanlagen" des BSI, hin. Nach dem bekannten Cyber-Angriff auf Norsk Hydro im März 2018 mit LockerGoga gab es im Januar 2019 mit der gleichen Ransomware Angriffe auf die französische Ingenieurgesellschaft Altran, die vor allem in der Technologieberatung tätig ist. Im März 2019 waren die beiden amerikanischen Chemieunternehmen Hexion, ein Produzent von Duroplastharzen und verwandten Spezialprodukten, und die Momentive Performance Materials, der weltweit zweitgrößte Hersteller von Silikon und Silikon-Derivaten, betroffen.

Über welche Wege finden die Angreifer ihre Ziele? Wiesner nennt als die wichtigsten Angriffspfade, die in den letzten Jahren mit wachsender Tendenz benutzt wurden:

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten.

Viele der Angriffe nutzen bis an den Leichtsinn grenzendes fehlendes Know-how und mangelnde Ausbildung aller Beschäftigten bezüglich Cyber Security. So beschreibt dann auch Erwin Kruschitz, Vorstand der Anapur, die Situation bildlich: „Aus meiner Wahrnehmung als Berater und Auditor kann ich sagen, dass die Security in der Prozessindustrie den Kinderschuhen entwächst. Über die Pubertät sind wir allerdings wohl auch noch nicht hinweg." Als wichtige Komponenten auf dem Weg zum erwachsen werden fordert er,

- Komponenten zu entwickeln, die Security bereits mitbringen d.h. nicht erst noch abgesichert werden müssen
- Vertrauensvolle Kommunikations- und Fehlerkultur zu leben, z.B. zwischen Herstellern und Anwendern oder zwischen Betroffenen und dem Rest der Community
- mehr Know-How aufbauen.

Entsprechend dieser Erkenntnis reagiert auch der Staat, so Kruschitz. Aktuell entsteht das IT-Sicherheitsgesetz in der zweiten Version mit Verschärfungen für Systemhersteller und Anwender. Das BSI entwickelt ein Grundschutzprofil für die Chemieindustrie. Das kann dazu beitragen, dass es eine deutschlandweite Harmonisierung der Security- Anforderungen geben wird. Aktuell variieren die Vorgaben noch in Abhängigkeit vom Bearbeiter beim jeweiligen Regierungspräsidium bzw. Gewerbeaufsichtsamt.

Das IT-Sicherheitsgesetz in der zweiten Version bringt Verschärfungen für Systemhersteller und Anwender.

Erwin Kruschitz, Anapur

Auf sein Bild mit den Heranwachsenden zurückkommend resümiert Kruschitz: „Gelassenheit ist sicher eine entscheidende Tugend von Eltern pubertierender Kinder. Im Gegensatz dazu gilt für den Bereich der Cybersecurity, dass ausschließlich proaktives Handeln aus der Adoleszenz führt. Dabei gibt es noch viel zu tun."

Volker Oestreich, CHEManager

- www.bsi.bund.de
- www.anapur.de
- www.videc.de