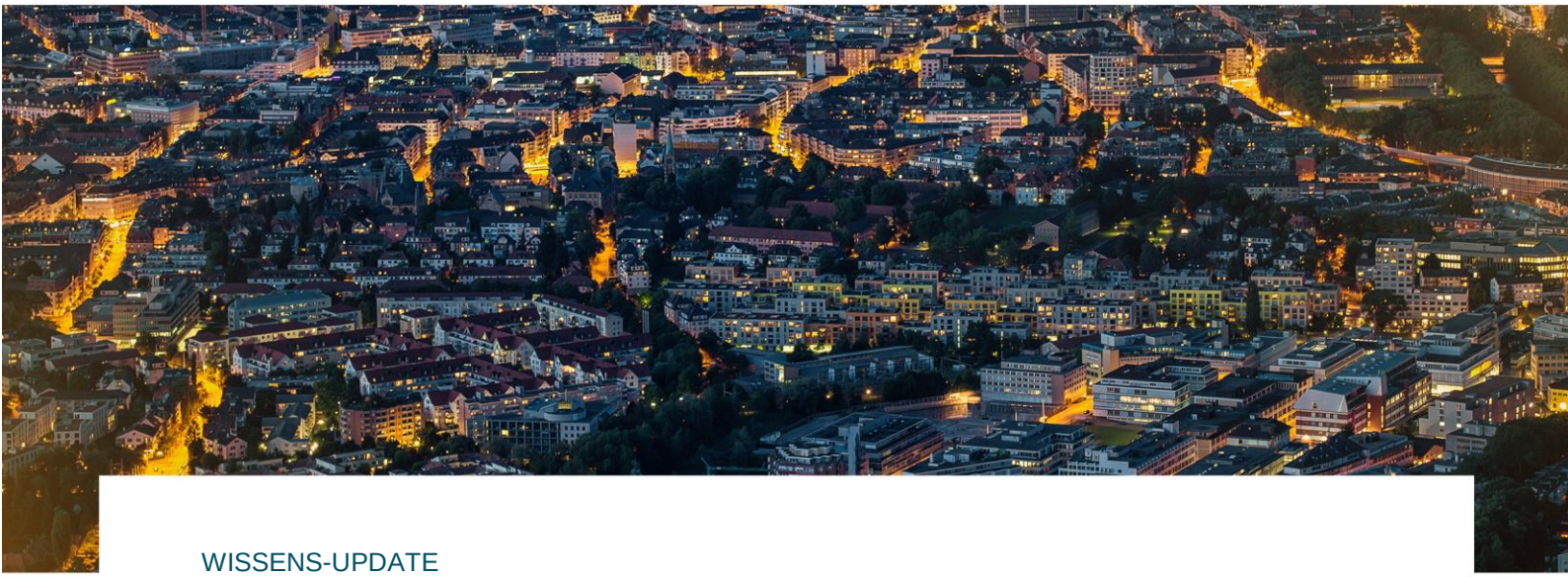
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

IoT-Sicherheit steht auch im Behördenumfeld im Fokus

CyOne Security | Steinhausen, 04. Oktober 2022

Das Internet of Things (IoT) wird die Gesellschaft in den nächsten Jahren grundlegend verändern. Auch im Behördenumfeld werden IoT-Technologien für einen Paradigmenwechsel sorgen. Die zunehmende Vernetzung der «Dinge» stellt die Informationssicherheit vor grosse Herausforderungen.

Das Internet of Things (IoT) verspricht eine Welt, in der alles mit allem vernetzt ist. In naher Zukunft werden nicht mehr nur Computer und Smartphones online sein. Vielmehr stehen alle möglichen «Dinge» in ständiger Verbindung mit dem Internet – von Uhren über Kleidung bis hin zu Autos. Möglich machen dies immer kleinere, günstigere und intelligentere Chips, die vermehrt auch in Haushaltsgeräte wie Kühlschränke und Toaster eingebaut werden.

Auch wenn das IoT noch in den Kinderschuhen steckt, so besteht doch bereits Gewissheit darüber, dass die umfassende Vernetzung der «Dinge» einen tiefschürfenden Wandel mit sich bringt. Das IoT wird nicht nur sämtliche Wirtschaftszweige umgestalten, sondern auch die Art und Weise wie wir leben: Im «Smart Home» kommunizieren Solarpanels, Heizung und Glühbirnen miteinander, um die Energie möglichst effizient zu nutzen. Und in der «Smart City» sammeln unzählige Sensoren eine Unmenge an Daten, anhand derer die Infrastruktur der Stadt laufend optimiert wird.

Milliarden von Sicherheitslücken

Da das IoT schon bald alle Schichten des Alltags durchdringen wird, befindet sich in Zukunft überall vernetzte IT – und diese ist leicht angreifbar. In der Regel sind Chips in smarten Alltagsgeräten nur ungenügend gesichert und können deshalb leicht gehackt werden. Die Sicherheitsrisiken von

vermeintlich harmlosen Produkten wie Kameras oder Router wurden in den letzten Jahren wiederholt deutlich. Wie einfach IoT-Geräte für Cyber-Attacken zweckentfremdet werden können, führte ein Hackerangriff im Oktober 2016 vor Augen: Die Schadsoftware Mirai infizierte zwei Millionen Geräte und nutzte diese, um Webseiten wie Amazon und Twitter lahmzulegen.

Bei einem Distributed Denial-of-Service-Angriff – wie im Fall der Software Mirai – bilden die infizierten Geräte ein Botnetz, um das Zielsystem mit vereinten Kräften anzugreifen. Das Zielsystem kann den grossen Ansturm nicht bewältigen und bricht zusammen. So wird jedes ungenügend gesicherte Gerät zu einem potenziellen Einfallstor für Hacker. Und der Pool an Schnittstellen wächst unaufhaltsam: Schätzungen gehen davon aus, dass 2020 rund 50 Milliarden Geräte mit dem Internet verbunden sein werden.

Die Armee der Zukunft Ist vernetzt

Wie im öffentlichen Sektor dürfte auch im militärischen Umfeld schon bald ein Netzwerk von Sensoren eingesetzt werden, um die Logistik effizienter zu gestalten. Die Vernetzung von eingesetztem Material und Lagerbeständen erlaubt es, Engpässe zu erkennen, bevor sie akut werden. Ohne eine aufwendige Inventur durchzuführen, kann jederzeit sichergestellt werden, dass alle Stützpunkte über die notwendigen Bestände verfügen.

Darüber hinaus ergeben sich für die Armee neue Möglichkeiten im Bereich der Wartung von Material und Fahrzeugen. Die sogenannte Predictive Maintenance (PM) ermöglicht ein vorausschauendes Instandhalten mittels intelligenter Datenanalysen. Die Vorteile liegen auf der Hand: Es kommt zu weniger Ausfällen und Unfällen, da die Sensoren Abnützungen frühzeitig erkennen. Materialengpässe sind ausgeschlossen, weil die smarte Logistik dafür sorgt, dass sich die Ersatzteile zur richtigen Zeit am richtigen Ort befinden. Und es können Kosten gespart werden, da das Material nicht mehr periodisch gewartet werden muss, sondern nur dann, wenn die Sensoren einen Wartungsbedarf melden.

Auch im Einsatz können IoT-Technologien einen grossen Nutzen stiften: Durch mit Sensoren ausgestattete Kleidung – sogenannte Wearables – kann der Gesundheitszustand von Soldaten in Echtzeit überprüft werden. Verschlechtert sich dieser, werden automatisch stabilisierende Massnahmen eingeleitet. Intelligente Sensoren können Soldaten – aber auch Einsatzkräfte der Polizei, Feuerwehr und Sanität – zudem potenzielle Gefahren aufzeigen und so vor Verletzungen bewahren. IoT-Technologien sorgen auch für mehr Übersicht: Drohnen versorgen Einsatzkräfte mit Video-Streams aus der Vogelperspektive.

In der Kriegsführung können digitale Sabotageakte schwerwiegende Folgen haben. Einerseits lassen sich über IoT-Technologien Fahrzeuge oder gar Waffen manipulieren. Zwei Sicherheitsforscher haben bereits 2015 eindrücklich aufgezeigt, wie einfach sich ein Jeep über vernetzte Bordelektronik fernsteuern lässt. Andererseits könnten durch die gezielte Manipulation von Geodaten Streitkräfte in eine Falle gelockt werden. Zudem bieten ungenügend gesicherte IoT-Technologien auch neue Angriffsflächen für Spionageakte. Durch Sicherheitslücken in der Kommunikation zwischen Soldat und Basis können aufschlussreiche Informationen über den Gegner gewonnen werden.

Die Bedeutung von IoT-Daten

Allen diesen neuen vernetzten Geräten ist gemeinsam, dass Sicherheit selten im Fokus steht. Das geht von den in der Cloud gespeicherten Daten über die Realisierung der Gerätefunktionen und des Zugriffsschutzes bis zur Sicherheit von Softwareupdates, falls solche überhaupt über längere Zeit verfügbar sind. Neben den Kosten ist der wohl wichtigste Grund dafür, dass sowohl Hersteller als

auch Benutzer die Bedeutung der anfallenden Daten und die damit verbundenen Risiken unterschätzen.

Denn diese Daten betreffen häufig nicht nur die eigentliche Anwendung, sondern liefern indirekt auch Informationen über das Umfeld, in dem das IoT-Gerät eingesetzt wird. So sagen die Ein- und Ausschaltzeiten einer Beleuchtung oder einer Heizung nicht nur aus, ob es hell oder warm ist, sondern geben auch Auskunft darüber, ob jemand vor Ort ist oder nicht. Transaktionsdaten von Getränke- und Snackautomaten erlauben personalisierte Profile über Tagesabläufe und sogar Hinweise auf Einsatzpläne. Anfang 2018 wurde bekannt, wie die von Fitnessuhren aufgezeichneten und öffentlich zugänglichen Joggingrouten die Position und Struktur geheimer militärischer Anlagen und Stützpunkte offengelegt haben.

Der Angreifer im eigenen Netz

Neben der Vertraulichkeit ist aber auch der Schutz des Zugriffs auf die IoT-Geräte zentral, vor allem bezüglich Konfiguration. Geräte mit nicht abgelösten Passwörtern oder mit Verbindung zu ungenügend geschützten Konten in der Cloud stellen geradezu eine Einladung für Angreifer dar.

Besonders wichtig ist die Integrität der Software von IoT-Geräten. Hier gibt es leider häufig Schwachstellen, die es Angreifern erlauben, modifizierte Software in die Geräte zu laden. Gründe dafür sind fehlende oder fehlerhaft realisierte Code-Signaturen und keine oder global eingesetzte Schlüssel zum Schutz von Updates.

Ist ein Angreifer einmal mit eigener Software in den Geräten, so kann er die Funktionen beliebig verändern und Sensoren aktivieren um Umgebungsdaten zu sammeln. Vor allem aber kann das Gerät zum Ausspähen der Netzwerkumgebung benutzt werden und dient somit als Ausgangspunkt für weitergehende Angriffe auf das interne Netz.

Überwinden von «Air Gaps»

Ein ganz anderes Risiko besteht im Zusammenhang mit offline betriebenen Systemen, die aus Sicherheitsgründen komplett von Netzen getrennt sind. Durch solche «Air Gaps» sollen diese Systeme vor Angriffen durch Malware geschützt oder zumindest das Abfliessen (Exfiltration) von Daten verhindert werden.

Angreifer können nun aber versuchen, eine «Air Gap» zu überwinden, indem sie Malware über Datenträger einschleusen und die Exfiltration über eine Ad-hoc-Verbindung zu einem ebenfalls manipulierten IoT-Gerät laufen lassen. Dazu kann fast alles dienen, was bei IoT-Geräten an Sensoren vorhanden ist. Die Malware kann zum Beispiel ein vorhandenes Wifi-Modul aktivieren und ein Ad-hoc-Netzwerk zum IoT-Gerät aufbauen. Oder sie kann Daten optisch über den Bildschirm oder eine LED aussenden und von einem IoT-Gerät via Kamera oder auch nur Helligkeitssensor empfangen lassen. Selbst eine akustische Übertragung ist prinzipiell möglich.

Diese Datenübertragungen können zudem so versteckt werden, dass sie unter normalen Umständen auch über längere Zeit nicht detektiert werden können. Je nach Kanal sind die erreichbaren Bandbreiten zwar klein, aber über längere Zeit können durchaus wertvolle Daten abfliessen.

Wie können Sie Ihre Organisation schützen?

Grundsätzlich sollten alle Prinzipien, die sich bezüglich Sicherheit bei ICT-Netzwerken, Software und Webtechnologien in den letzten Jahrzehnten durchgesetzt haben, auch bei IoT-Geräten angewendet werden. Die konsequente Verschlüsselung vertraulicher Daten spielt weiterhin die zentrale Rolle. Gegen Manipulationsversuche und Spionageakte hilft nur eine hochsichere Verschlüsselung, welche unter vollständiger Kontrolle der eigenen Organisation bleibt.

Der Ausgangspunkt ist die Awareness, das Kennen und Akzeptieren der möglichen Risiken und Konsequenzen beim Einsatz von IoT-Geräten in den eigenen Netzen und Räumlichkeiten. Daraus müssen Richtlinien und Prozesse abgeleitet werden, wie solche Geräte eingesetzt, integriert und verwaltet werden. Dazu gehören Vorgaben:

- zur Beschaffung von IoT-Geräten mit besonderem Augenmerk auf die Vertrauenswürdigkeit und Zuverlässigkeit der Hersteller
- zur kontrollierten Einbindung von IoT-Geräten in interne Netze, mit möglichst limitiertem Netzwerk- und Internetzugriff und der Verhinderung «lateraler» Verbindungen im internen Netz
- zur regelmässigen Wartung mit Firmware-Updates und -Patches

Bei Offlinearbeitsplätzen und -rechnern mit besonders kritischen Daten müssen trotz «Air Gap» zwingend die regelmässigen Updates von Betriebssystemen, Anwendungen und Anti-Malware Tools eingespielt werden.

Im IoT-Umfeld kommt erschwerend hinzu, dass die vernetzten Geräte unterschiedlich leistungsfähig sind, was bezüglich der Verschlüsselung gewisse Einschränkungen mit sich bringt. Bei hochwertigen IoT-Geräten können Algorithmen für die Verschlüsselung eingebaut werden. Bei leistungsschwächeren Geräten, zum Beispiel bei günstigen Sensoren, ist dies hingegen kaum möglich. Eine weitere Herausforderung sind die Übertragungsverfahren von IoT-Geräten: IoT-Geräte kommunizieren über Drahtlosprotokolle wie Zigbee, LoRaWAN, Bluetooth oder WLAN, und dabei kommen in der Regel statische Schlüssel zum Einsatz, die für alle Benutzer einheitlich sind und sich deshalb von Hackern relativ leicht abgreifen lassen.

Neben der Verschlüsselung der vertraulichen Daten ist auch die Authentifizierung entscheidend: Wer oder was hat wann Zugriff auf welche Daten? Und wie lässt sich verhindern, dass ein Unbefugter die Steuerung übernimmt? Hier gilt für IoT-Technologien, was in anderen Bereichen wie dem Onlinebanking schon seit langem gang und gäbe ist: Es braucht eine starke Authentifizierung über zwei oder mehrere Faktoren. Zudem muss das System Manipulationsversuche frühzeitig erkennen.

CyOne Security ist der vertrauensvolle Partner für IoT-Sicherheit

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security AG. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute noch, Ihre vernetzten Dinge vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Produkte und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.