INDUSTRIE 4.0
ÖSTERREICH

CYBER-SECURITY LEITFADEN FÜR PRODUKTIONSBETRIEBE

SCHUTZ VOR CYBERATTACKEN – MEHR WERTSCHÖPFUNG MIT SECURITY

Verein Industrie 4.0 Österreich

INHALTSVERZEICHNIS

VORWORT 5

1. EINLEITUNG 6

2. INFEKTION MIT SCHADSOFTWARE ÜBER INTERNET UND INTRANET IM PRODUKTIONSBEREICH 8
   - 2.1 Industrie 4.0 – IT und OT 9
   - 2.2 Schutz- und Gegenmaßnahmen 10
   - 2.3 Beispiel einer Schadsoftware 11

3. MITARBEITERINNEN ALS RISIKOFAKTOR 12
   - 3.1 Angriffsbeispiele 14
   - 3.2 Schutz- und Gegenmaßnahmen 16

4. DOS- UND DDOS-ANGRIFFE 18
   - 4.1 Motivation für DDoS-Angriffe 19
   - 4.2 Mögliche Schäden 19
   - 4.3 Schutz- und Gegenmaßnahmen 20
   - 4.4 Beispiele von DDoS-Angriffen 20

5. GEFÄHRDUNG DURCH FERNWARTUNG 22
   - 5.1 Schutz- und Gegenmaßnahmen 23

6. CLOUD SECURITY – KOMPROMITTIERUNG VON EXTRANET UND CLOUD-KOMPONENTEN 26
   - 6.1 Abhängigkeit der Produktion von einem Extranet- und Cloud-Dienst 27
   - 6.2 Unzureichende Mandantentrennung in Cloud-Plattformen 29

7. VERLETZUNG DES DATENSCHUTZES DURCH IT-SICHERHEITSLÜCKEN 30
   - 7.1 Meldepflicht bei Datenschutzverletzungen 31
   - 7.2 Schutz- und Gegenmaßnahmen 31

8. CYBER-SECURITY HOTLINE 0800 888 133 32
   - 8.1 Security Hotline 33
   - 8.2 Ansprechpersonen in den Bundesländern 34
   - 8.3 Kooperation mit staatlichen Stellen und Organisationen/Vereinen 34
   - 8.4 Statistik 34

9. ANHANG 36
   - 9.1 Schadsoftware 37
   - 9.2 Abkürzungen 38
   - 9.3 Glossar 38

10. LITERATUR 40

11. WEITERFÜHRENDE LINKS 42

12. DANK 44

IMPRESSUM 46

Geschätzte Leserinnen und Leser!
Liebe Mitglieder der Plattform Industrie 4.0!

Die umfassende Digitalisierung von mittlerweile fast allen Bereichen in unserer Gesellschaft hat in einem atemberaubenden Tempo die Spielregeln der Wirtschaft aber auch in vielen Facetten Mechanismen unseres Zusammenlebens verändert. Digitale Kommunikationssysteme bestimmen unseren Alltag und der Digitalisierungs- und Transformationsprozess bekommt durch die gerade begonnene Vernetzung unserer vielen physischen Objekte zu einem Internet der Dinge (IoT – Internet of Things) eine neue Dynamik.

Diese Dynamik erfasst nun auch unsere Produktionsbetriebe bzw. alle UnternehmerInnen. Der Einsatz von Computern und Software in all unseren Maschinen, die globale Vernetzung unserer Systeme und die Wichtigkeit von Daten für unsere Geschäftsmodelle und Geschäftsprozesse werden zu bestimmenden Elementen einer wettbewerbsfähigen Geschäftsstrategie. Dieser durch die Digitalisierung getriebene Wandel zur sogenannten Industrie 4.0 stellt jeden einzelnen von uns vor neue Herausforderungen.

Die Digitalisierung unserer Maschinen bringt neben Produktivitätssteigerung, Qualitätsverbesserung, Vereinfachungen von Abläufen und Bequemlichkeit für den Kunden auch eine große Problematik mit sich: steigende Sicherheitsrisiken für unsere Systeme aber auch für die generierten Daten. Kundendaten, Patente, Verfahrensregeln werden für den Konkurrenten interessante Angriffsziele, verletzliche Systeme und kritische Infrastrukturen werden potentielle Ziele von Terroristen, oder ganze Unternehmen werden zur Zielscheibe der organisierten Kriminalität. Durch die Digitalisierung und durch die globale Vernetzung steigen einerseits die Chancen, wirtschaftlich erfolgreich zu sein, andererseits werden die Bedrohungsszenarien immer größer und können für jedes einzelne Unternehmen auch zur potentiellen Überlebensfrage werden.

Neben der Feststellung der neuen Bedrohungslage durch die Digitalisierung sollten wir allerdings auch die neuen Möglichkeiten erkennen, um durch Kompetenz und geschickt eingesetzte Technik einen Wettbewerbsvorteil unserer Unternehmen zu erzielen. Schutz von privaten Daten, sichere und höchst zuverlässige Produkte und sichere Produktionen werden schlussendlich im globalen Wettbewerb einen wesentlichen Beitrag für entsprechende USPs ausmachen und sollten daher von jedem österreichischen Unternehmen als fixer Bestandteil in der Produkt- und Standortstrategie verankert sein. Führende Cyber-Security-Technologien „Made in Austria“ sind vielfach durch innovative österreichische Unternehmen vorhanden und bilden die Grundlage, um österreichische Innovationen auch im digitalen Zeitalter global erfolgreich zu vermarkten.

Diese Broschüre soll Ihnen einen Überblick über aktuelle Bedrohungsszenarien geben und eine erste Anleitung vermitteln, wie man am Ende einfach zu einem sicheren digitalen System gelangen kann, um am globalen Markt der Zukunft auch nachhaltig bestehen zu können. Mit dieser Zielsetzung werden dem Leser in leicht verständlicher Weise weit verbreitete Angriffsmethoden wie DDoS-Attacken, Ransomware und Methoden zum Einschleusen von Schadsoftware, Bedrohungen bei Wartungszugriffen über das Internet aber auch die mögliche Gefahr durch die eigenen MitarbeiterInnen im Unternehmen erklärt. Eine Übersicht über erfolgte Angriffe auf die österreichischen Betriebe im Jahr 2018 und eine erste Checkliste für Cyber-Sicherheit runden die Informationen ab und sollen eine erste Hilfestellung für jedes Unternehmen darstellen.

Zusammenfassend ist es wichtig festzuhalten, dass sich kein Unternehmen als zu klein und aus globaler Sicht zu unbedeutend einschätzen darf, um für die Cyber-Crime-Industrie nicht doch interessant zu sein. Cyber-Kriminalität sowie Wirtschafts- und Industriespionage mit hoch entwickelten Angriffskenntnissen kann nur mit effektiven Schutzmaßnahmen entgegengewirkt werden.

DI Dr. Wilfried Enzenhofer, MBA

EINLEITUNG

1

In der vorliegenden Broschüre wird anhand von einfachen Beispielen und Zusammenfassungen ein erster Überblick über die Thematik Cyber-Security im Produktionsbereich zur Verfügung gestellt. Das Ziel der vorgestellten Beispiele und Szenarien, welche alle aktuellen Beispielen aus der Praxis entsprechen, ist es zu zeigen welche Bedeutung ein unzureichendes Bewusstsein dieser Thematik für einen Produktionsbetrieb haben kann. Neueste Statistiken zeigen, dass Österreich zu den Top fünf Angriffszielen weltweit gehört. [1.1] Beschreibungen von Bedrohungsszenarien aber auch erste Ansätze von Lösungsvorschlägen sollen dem Leser eine Hilfestellung bieten, um weitere konkrete Schritte planen und implementieren zu können.

Im Abschnitt 2 werden die grundsätzliche Thematik von Schadsoftware und die Problematik in IT-Systemen und Produktionssystemen diskutiert. In Abschnitt 3 wird darauf eingegangen welche Rolle der Mensch als Benutzer bzw. als Mitarbeiter im IT-Sicherheitsbereich im Unternehmen einnimmt, in Abschnitt 4 wird die Bedrohung von DDoS-Angriffen erklärt und in Abschnitt 5 wird die besondere Gefährdung durch schlecht geschützte Fernwartungszugänge auf Produktionsmaschinen thematisiert. Abschnitt 6 behandelt die neue Herausforderung von Daten und IT-Sicherheit bei Cloud-Lösungen und in Abschnitt 7 wird die Problematik der Verletzung des Datenschutzes durch Sicherheitslücken diskutiert. Abschließend wird in Abschnitt 8 ein neues Service für österreichische Klein- und Mittelbetriebe vorgestellt: die Cyber-Security Hotline der Wirtschaftskammer Österreich mit einer Übersicht über erfolgte Angriffe auf die österreichischen Betriebe im Jahr 2018. Eine Zusammenstellung wichtigster Begrifflichkeiten und Erläuterungen in diesem Kontext und eine erste Checkliste für Cyber-Sicherheit rundet die Informationen ab und soll eine erste Hilfestellung für jeden interessierten Leser/jede interessierte Leserin darstellen.

VEREIN INDUSTRIE 4.0 – DIE PLATTFORM FÜR INTELLIGENTE PRODUKTION

Der Verein „Industrie 4.0 Österreich“ wurde 2015 als Initiative des österreichischen Bundesministeriums für Verkehr, Innovation und Technologie sowie von Arbeitgeber- und Arbeitnehmerverbänden gegründet. Diese erarbeiten gemeinsam mit Mitgliedern aus Wirtschaft, Wissenschaft und Interessenvertretungen in spezifischen ExpertInnengruppen Strategien zur nachhaltigen und erfolgreichen Umsetzung der digitalen Transformation im Kontext von Industrie 4.0. Ziel ist es, die technologischen Entwicklungen und Innovationen durch Digitalisierung bestmöglich und sozialverträglich für Unternehmen, Beschäftigte und die Gesellschaft in Österreich zu nutzen und verantwortungsvoll umzusetzen. Der Verein Industrie 4.0 Österreich nimmt dabei eine wichtige Rolle in der nationalen und internationalen Koordinierung, Strategiefindung und Informationsbereitstellung ein.

EXPERTINNENGRUPPE SECURITY UND SAFETY

Für die erfolgreiche Umsetzung von Industrie 4.0 und der umfassenden Vernetzung von Wertschöpfungsketten ist eine zuverlässige, hochverfügbare und dauerhaft sichere Nutzung von weltweit vernetzten Maschinen und Anlagen sowie von innovativen, datengetriebenen Technologien unabdingbar. Manipulation, Zugriffe auf sensitive Informationen bis hin zu gezielten und hochspezialisierten Cyberangriffen stellen nur einige der Bedrohungen dar, wodurch die Aufrechterhaltung von IT- und OT Sicherheit (security) als auch der funktionale Sicherheit (safety), Zuverlässigkeit und rechtliche Sicherheit von Systemen zu einer zentralen Herausforderung für Gesellschaft und Wirtschaft werden.
Mit der Einrichtung der Arbeitsgruppe Security und Safety möchte die Plattform Industrie 4.0 Österreich die Wahrnehmung um die Wichtigkeit und Bedeutung des Themas Sicherheit für Industrie 4.0 erhöhen, relevante Akteure in Österreich vernetzen und dazu beitragen Security & Safety als österreichischen Wettbewerbsvorteil zu etablieren. VertreterInnen von universitären wie auch außeruniversitären Forschungseinrichtungen, Politik und Verwaltung, Unternehmen und Interessensvertretungen fungieren dabei als zentrales Steuerungsgremium und legen Arbeitsschwerpunkte und die inhaltliche Ausrichtung der Aktivitäten der Plattform Industrie 4.0 im Bereich „Security und Safety“ fest.

INFEKTION MIT SCHADSOFTWARE ÜBER INTERNET UND INTRANET IM PRODUKTIONS-BEREICH

2

2.1 INDUSTRIE 4.0 – IT UND OT

Für eine erfolgreiche Umsetzung des Themas Industrie 4.0 im Unternehmen, müssen entsprechende Sicherheitsaspekte von Anfang an in das Systemdesign einbezogen werden. Vor allem die besondere Charakteristik produzierender Unternehmen, welche üblicherweise durch zwei verschiedene Systembereiche gekennzeichnet ist – die IT für die üblichen Geschäftsprozesse (Office-IT) und die IT für die verschiedenen Produktionsanlagen – Produktionstechnologie oder auf Englisch „Operational Technology" (OT) – bringt spezifische Herausforderungen für das Systemdesign und für die Betriebsprozesse.

Die Schutzziele der Informationssicherheit wurden in den Bereichen Information Technology (IT, Informationstechnologie) und Operational Technology (OT, Produktionstechnologie) wie z.B. industrielle Steuerungssysteme bislang separat sowie mit unterschiedlicher Priorität verfolgt. Ausschlaggebend dafür ist, dass IT- und OT-Systeme angesichts ihrer Charakteristika ein unterschiedliches Maß an Sicherheit erforderten. So wurde etwa bei OT der Fokus primär auf Verfügbarkeit und Zuverlässigkeit gelegt. Bei klassischen Systemen aus der Business-IT haben Vertraulichkeit und Integrität der Daten üblicherweise den Vorrang. OT-Systeme beruhen oftmals auf proprietären Technologien und folgten mitunter oft lediglich dem Prinzip „security through obscurity" (Sicherheit durch Unklarheit für den Angreifer). Daher war die strikte Abtrennung der industriellen Steuerungssysteme vom Internet ein notwendiges Minimum an umzusetzenden Sicherheitsmaßnahmen [2.1]. Mit der stetigen Vernetzung der Systeme durch Industrie 4.0 Konzepte und dem Internet der Dinge (IoT) verschwimmen die Grenzen zwischen IT und OT jedoch immer mehr und inhärent unsichere industrielle Steuerungssysteme werden direkt an das Internet angebunden und es entsteht eine technische Verbindung vom Unternehmensnetz mit dem Produktionsnetz. Demzufolge sind Produktionssysteme zunehmend Cyberangriffen ausgesetzt. Diese können nun sowohl über Internet als auch vom Unternehmensnetz aus dem Intranet erfolgen. Der Trend zur steigenden Bedrohungslage lässt sich auch anhand der jährlich wachsenden Sicherheitsvorfälle, die den Behörden gemeldet werden, erkennen. So wurden im Jahr 2010 in den USA nur 39 Sicherheitsvorfälle in kritischen Infrastrukturunternehmen bearbeitet, während es 2016 bereits 290 waren [2.2, 2.3].

Zusammenfassend kann man festhalten, dass drei wichtige Aspekte den OT-Bereich vom IT-Bereich unterscheiden:

- **Safety versus Security:** Unter **Safety** versteht man die Betriebssicherheit von Systemen um Schaden an Menschen und Sachen zu verhindern. Sie hat in der Produktion höchste Priorität, da hier bei Falschbedienung oder Funktionsfehlern von Maschinen Menschenleben gefährdet sein oder hohe Sachkosten entstehen können. Security beschreibt den Schutz vor unerlaubten Zugriffen auf technische Systeme durch kriminelle Absichten und hatte bisher vorwiegend in der Office-IT eine Bedeutung. Durch das fortlaufende Zusammenwachsen von Office-IT und Produktions-IT nimmt auch die Cyber-Security eine immer wichtigere Rolle ein, da auch Anlagen und Systeme zunehmend ein Angriffsziel sind.

  Erschwert wird die Einführung von Cyber-Security-Maßnahmen in der Produktionsumgebung dadurch, dass die Bereiche von Produktions-IT und Office-IT unterschiedliche Schutzziele verfolgen. Während in der Produktions-IT die ständige Verfügbarkeit höchste Priorität hat, sind kurze Ausfälle in der Office-IT noch akzeptabel. Dafür darf in der Office-IT das Schutzziel der Vertraulichkeit nicht verletzt werden, welches bei der Produktion eher nachrangig ist.

- **Mangelndes Cyber-Sicherheitsbewusstsein in der Produktions-IT (OT):** Während der Einsatz von Sicherheitsmaßnahmen im Bereich der Informationstechnologie (IT) bereits seit Jahren übliche Praxis ist, sind diese für den Bereich der Produktions-IT (OT) noch nicht selbstverständlich. Bisher gab es oft keine Notwendigkeit von besonderen Security Maßnahmen da Produktionsanlagen entweder nicht digitalisiert waren oder keine Anbindung an das Internet hatten. Dadurch ist auch das notwendige Bewusstsein bei den verantwortlichen Personen oft nicht besonders ausgeprägt. Und im Industriebereich werden z.B. oft aus praktischen und Bequemlichkeitsgründen Standard-Passwörter verwendet, welche selbst von unerfahrenen Kriminellen einfach ausfindig gemacht werden können.

Darüber hinaus ist es wichtig zu beachten, dass es einfache und öffentlich verfügbare Werkzeuge gibt, um Geräte mit solchen Sicherheitsproblemen einfach ausfindig zu machen. Beispielsweise können mit der Suchmaschine Shodan (www.shodan.io) Geräte, welche über das Internet erreichbar sind, wie WLAN-Router, Kühlschränke oder Kameras, Heizungssteuerungen aber auch komplette Industrieanlagen, gefunden werden, welche ungeschützt oder nur mit Standardpasswörtern, Industrieeinstellungen, oder auch allgemein bekannten Passwörtern geschützt sind. Für jemanden mit kriminellen Absichten ist es dann leicht, sich Zugriff auf ein solches System zu verschaffen.

Auch werden externe Dienstleister oder Hersteller oft nicht als potentiell gefährdend wahrgenommen und dadurch werden notwendige Sicherheitsmaßnahmen oft vernachlässigt. Es gilt auch zu beachten, dass interne wie externe Mitarbeiter in Unternehmen oft einfach Zugriff zu Produktionsanlagen und zum Firmennetz haben und dadurch – beabsichtigt wie unbeabsichtigt – Maschinen und IT-Systeme des Unternehmens mit Schadsoftware infizieren können (siehe Abschnitt 3).

› **Veraltete Architektur:** Viele Firmen arbeiten noch mit einer flachen und damit unsicheren Netzarchitektur, wodurch sich eingeschleuste Schadsoftware leicht in einem Netzwerk ausbreiten kann. Viele der Produktionsanlagen sind außerdem direkt mit dem Internet verbunden, oft einfach nur aus Bequemlichkeit oder aus Unwissenheit.

2.2 SCHUTZ- UND GEGENMASSNAHMEN

Industrielle Steuerungssysteme können vor einer Infektion mit Schadsoftware, die von Internet oder Intranet ausgeht, mit folgenden Sicherheitsmaßnahmen geschützt werden:

1. Es sollte auf eine geeignete Segmentierung des Netzwerks geachtet werden, um nach dem Defense-in-Depth-Konzept eine vielschichtige Sicherheitsarchitektur zu erzielen. Dadurch sind OT-Komponenten vom Unternehmensnetzwerk angemessen abgeschottet und können nicht einfach über das Internet erreicht werden. Das gesamte Netzwerk der Produktion wird dabei anhand der darin befindlichen Dienste und deren Schutzbedarf in Zonen aufgeteilt. Diese Zonen bilden sogenannte Automatisierungszellen, die mit technischen Sicherheitsmaßnahmen, wie etwa Firewalls, abgesichert werden [2.4]. Dank dieser Vorgehensweise können auch die Zonenübergänge konsequent kontrolliert werden, um somit den Netzwerkverkehr zwischen Segmenten zu überwachen. Neben dem Einsatz von Firewalls für die Zonierung können auch spezielle technische Einrichtungen (Datendioden) betrieben werden, um einen Datentransport in nur eine Richtung sicherzustellen. Um das Industrienetzwerk für die Segmentierung in logische Ebenen (Level) zu untergliedern, kann das Purdue-Modell[1] [2.5] herangezogen werden. Darauf aufbauend, ist gemäß der IEC 62443-3-2 das Netzwerk in Zonen und Zonenübergänge zu unterteilen.

2. Die Angriffsfläche, d.h. die Möglichkeit um über potentielle Schwachstellen einen Zugang zu Systemen zu erlangen, muss so klein wie möglich gehalten werden. Eine solche Reduktion der Angriffsfläche erfolgt indem beispielsweise ungenutzte Funktionalitäten von Systemen deaktiviert werden. Des Weiteren sollten vorkonfigurierte Benutzerkonten, die beispielsweise nur mit Standardpasswörtern geschützt sind, entfernt werden. Schließlich ist die Implementierung eines durchdachten Berechtigungskonzepts zielführend, um einen Zugriff von Benutzern ausschließlich auf die jeweils unbedingt erforderlichen Dienste zu beschränken.

3. Bekannte Schwachstellen von IT-Systemen sollten durch laufende Aktualisierungen der Software behoben werden. Diese sollten allerdings vor Ausrollung in einer Testumgebung überprüft werden, um mögliche neue Fehlerzustände der Produktionssysteme zu vermeiden.

[1] Das Purdue-Modell ist eine generische Architekturbeschreibung und Methode zur Absicherung für industrielle Steuerungsanlagen (ICS).

4. Zu guter Letzt sollten OT-Systeme umfassend mittels Monitoringsystemen überwacht werden, um sicherheitsrelevante Ereignisse möglichst frühzeitig zu erfassen und wenn notwendig auch verantwortliche Personen zu alarmieren um potentielle Angriffe frühzeitig abwehren zu können.

2.3 BEISPIEL EINER SCHADSOFTWARE

Seit 2011 ist die Schadsoftware BlackEnergy2 im Umlauf [2.6]. BlackEnergy2 nützt speziell vorhandene Schwachstellen von Benutzerschnittstellen[2] (HMI Human-Machine Interface) von Systemen in Produktionsanlagen, die direkt mit dem Internet verbunden sind.

Durch solche Fernzugänge über das Internet, welche oft für Fernwartungen eingerichtet werden, erhalten auch potentielle Angreifer die Möglichkeiten, einen direkten Zugang zu Anlagensteuerungen zu bekommen. Diese Problematik wird in Kapitel 5 noch im Detail behandelt. Dadurch können potentiell gezielte Manipulationen der Steuerungssysteme vorgenommen werden.

Bei einem geschickten Cyberangriff auf eine Produktionsanlage ist auch eine Verschleierung der Manipulationen möglich, indem beispielsweise Zustände des Anlagenprozesses an Anzeigesystemen vorgetäuscht werden, damit die Manipulation an der Anlage durch das Betriebspersonal nicht erkannt werden kann.

Obwohl Angriffe mittels BlackEnergy2 nur auf Spionage abzielten [2.7], können Infektionen mit dieser Schadsoftware durchaus auch substantielle negative Auswirkungen auf die Funktionsfähigkeiten von ganzen Anlagen haben. Die schwerwiegenden Folgen eines Angriffs durch die Schadsoftware BlackEnergy3, welcher der Nachfolger von BlackEnergy2 ist, auf industrielle Steuerungssysteme wurde im Dezember 2015 deutlich. Die Angreifer drangen mithilfe dieser Schadsoftware in das Unternehmensnetz ukrainischer Energieversorger ein und gelangten von dort in das Produktionsnetz [2.7]. Auf diese Weise wurden mehr als 225.000 Haushalte in der Ukraine für sechs Stunden vom Strom abgeschnitten [2.7]. Großflächig erzeugte Blackouts durch Cyberangriffe (Cyber-Blackouts) werden somit zur Realität.

Der Gefahr von solchen Cyberangriffen sind jedoch nicht nur Energieversorger ausgesetzt, sondern sie stellen eine Bedrohung für alle Produktionsunternehmen dar.

[2] Eingabemasken, Bedienoberflächen, Graphiken, Anzeigetafeln, etc.

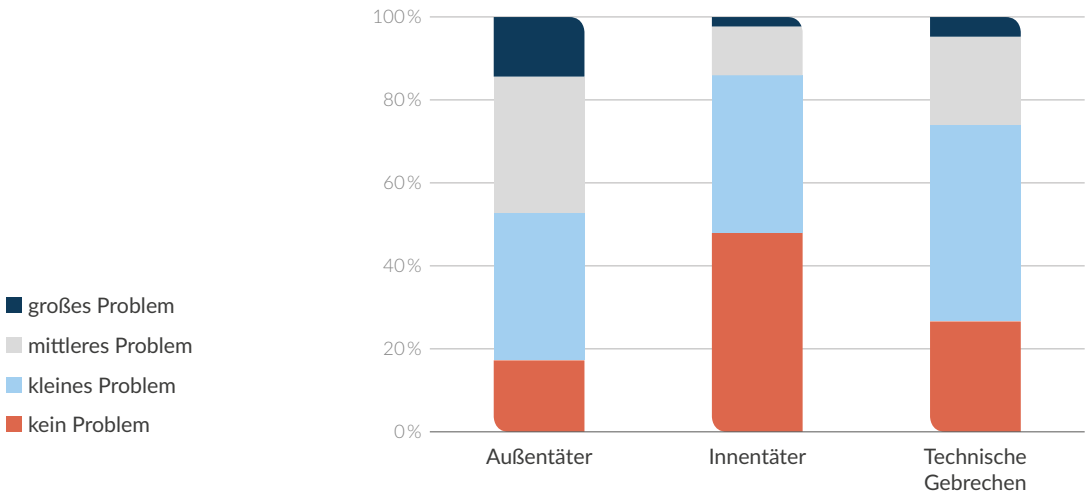
MITARBEITER-INNEN ALS RISIKOFAKTOR

3

MitarbeiterInnen nehmen bei ihrer täglichen Arbeit mit betrieblichen IT-Systemen oder an technischen Maschinen eine bedeutende Rolle für den sicheren Umgang mit schützenswerten Informationen und Systemen ein. MitarbeiterInnen setzen dabei manchmal bewusste Handlungen, aber handeln oft auch ganz unbewusst und tragen so zu Sicherheitsvorfällen bei. Das schnelle Öffnen eines Mailanhanges mit Schadsoftware, die nicht autorisierte Informationsweitergabe am Telefon oder das fehlende Bewusstsein über technische Gefahren im Arbeitsalltag können schon der Beginn eines Cyberangriffes sein. Dieses führt in weiterer Folge zum Verlust schützenswerter Informationen, zu finanziellen Schäden oder zu einer Beeinträchtigung der Reputation des Unternehmens. Daher sind Sensibilisierung, Schulung und das Schaffen von entsprechendem Bewusstsein bei MitarbeiterInnen entscheidende Kriterien für mehr Sicherheit in der technischen Infrastruktur von Unternehmen.

So weist der jährlich erscheinende Cyber-Sicherheitsbericht der österreichischen Bundesregierung – wie in Abbildung 3.1 „Cyber-Sicherheitsvorfälle in österreichischen Unternehmen" verdeutlicht – neben technischen Gebrechen und Außentätern – auch auf Sicherheitsvergehen durch interne MitarbeiterInnen hin [3.1]. Offen bleibt jedoch, in welchem Verhältnis das aktive Sabotieren der betrieblichen Infrastruktur oder das Ausspionieren vertraulicher Informationen zu unbewusstem oder fahrlässigem Verhalten steht.

Abbildung 3.1: CYBER-SICHERHEITSVORFÄLLE IN ÖSTERREICHISCHEN UNTERNEHMEN, EINSCHÄTZUNG VON VORFALLSURSACHEN 2018



3.1 ANGRIFFSBEISPIELE

Im Folgenden sind vier Beispiele von Cyberangriffen zusammengefasst, welche wesentlich auf das Fehlverhalten von Menschen aufbauen.

CEO-FRAUD

„CEO-Fraud" bedient sich einer ‚internen' Variante des Rechnungsbetruges. Hier geben sich Angreifer als Teil des Unternehmens – z.B. als Geschäftsführer oder Finanzvorstand – aus und fordern von MitarbeiterInnen, oft unter Hinweis auf die notwendige Geheimhaltung, eine dringende Überweisung, beispielsweise durch eine gefälschte E-Mail an die Buchhaltung [3.2].

Der Fall eines oberösterreichischen Unternehmens, das durch betrügerisches Handeln Unbekannter einen mittleren zweistelligen Millionenbetrag verlor, wurde im Jänner 2016 durch Medienberichte [3.3] bekannt. Dies führte im konkreten Fall zu personellen Maßnahmen. Die betrieblichen Verantwortlichen mussten das Unternehmen verlassen. Auch Schadenersatzansprüche aufgrund der Nichteinhaltung betrieblicher Entscheidungsabläufe können eine Folge sein.

SCHAD- UND VERSCHLÜSSELUNGSSOFTWARE DURCH PHISHING EMAILS

Cyberangriffe durch Schadsoftware in Mailanhängen haben massiv zugenommen. Oft öffnen MitarbeiterInnen eine auf den ersten Blick unauffällige Mail. Eine beliebte Methode war und ist immer noch über E-Mails zu vermeintlich fehlgeschlagenen DHL-Sendungen Schadsoftware in betriebliche Systeme einzubringen. Das Öffnen eines Mailanhanges mit der Kurzinfo *„Ihr DHL Paket konnte nicht zugestellt werden. Weitere Informationen im Anhang …"* führt dazu, dass ein im Anhang mitgesandter Computervirus sich am verwendeten Computer installiert. Dieser breitet sich im Netzwerk aus, sammelt Informationen ein und verschlüsselt auch Dateien um Erpressungen durchzuführen zu können. Wird die Schadsoftware nicht durch technische Schutzmaßnahmen wie Firewall oder Virenscanner abgewehrt, sind die negativen Folgen oft beträchtlich.

Der weltweite Cyberangriff mit der Verschlüsselungssoftware *„WannaCry"* hat in den letzten Jahren beträchtlichen Schaden in Unternehmen angerichtet. In einem Hotel in Südösterreich [3.4] breitete sich dieser Virus im gesamten Haus aus und verschlüsselte alle Geräte und sogar die elektronischen Schlösser der Zimmertüren, die Gäste konnten ihre Zimmer nicht mehr mittels Chipkarte betreten. Das betroffene Unternehmen sah sich gezwungen, an die Erpresser Lösegeld zu zahlen, um wieder Zugriff auf die eigenen Systeme zu erhalten.

Der Hotelchef erläuterte dazu [3.4]: „Das Haus war mit 180 Gästen total ausgebucht, wir hatten keine andere Chance. Weder Polizei noch Versicherung helfen einem in diesem Fall. Die Wiederherstellung unseres Systems nach der ersten Attacke im Sommer hat uns mehrere Tausend Euro gekostet. Von der Versicherung bekamen wir bis heute kein Geld, da kein Täter ausgeforscht werden konnte."

EINSCHLEUSEN VON SCHADSOFTWARE DURCH MITARBEITERINNEN

Angriffe auf Industrieunternehmen durch Infektion mit Schadsoftware wie Viren oder Trojaner sind laut BSI Analyse [3.5] die zweithäufigste Angriffsform hinter Social Engineering Angriffen wie Phising Emails. Häufig geschieht dies durch den Einsatz von Wechselmedien wie beispielsweise USB-Sticks. Dadurch erfolgt ein Angriff von innen aus dem eigenen Unternehmensbereich. Ein Paradebeispiel dafür ist der Angriff auf die iranischen Atomanlagen durch Stuxnet. Dabei wurde eine speziell auf die zu attackierende Infrastruktur angepasste Schadsoftware entwickelt und über präparierte USB-Sticks in das System eingeschleust.

Dass für einen solchen Angriff oftmals gar keine böse Absicht eines Mitarbeiters vorhanden ist, um ein Industrieunternehmen zumindest teilweise lahmzulegen, veranschaulicht folgendes Beispiel.

Der Produktionsmitarbeiter eines Hightech-Unternehmens in Österreich war in der Nachtschicht tätig. Als sich der Akku seines Mobiltelefons dem Ende zuneigte und er jeden Moment

den Anruf seiner Frau erwartete, die ihr erstes Kind bekam, beschloss er mangels Ladegerät das Datenkabel an der USB-Buchse des Fertigungs-PCs anzuschließen. Eine knappe Stunde später, in den frühen Morgenstunden kam es zu einem plötzlichen Stillstand des Fräszentrums.

Eine auf seinem Mobiltelefon gespeicherte Schadsoftware hatte die Steuerung der Fräße über die USB-Schnittstelle des Industrie-PCs infiziert und nutzte die Hotspot-Fähigkeit des Smartphones, um zusätzlich mit einer Angriffs-Software über das Internet in Verbindung zu treten. Dem Produktionsmitarbeiter war nicht bewusst, dass die USB-Schnittstelle sehr leicht missbraucht werden kann.

Das Unternehmen reagierte rasch und investierte in die Erstellung und Umsetzung eines Sicherheitskonzepts, das speziell auf die Bedürfnisse der Produktion Rücksicht nahm. [3.6]

ANGRIFFE DURCH SOCIAL ENGINEERING

Folgendes Beispiel soll einen typischen Cyberangriff mit Social Engineering Methoden verdeutlichen.

Drei Studenten einer technischen Hochschule hatten sich für ihre Seminararbeit „Aufbau und Sicherheit von Produktionsnetzwerken" ein besonderes Ziel ausgesucht, eine nahe ihrem Wohnort gelegene Keksfabrik. Nachdem das Sicherheitskonzept dieser Firma aus nachvollziehbaren Gründen weder öffentlich zugänglich ist noch auf Anfrage der Studenten bekanntgegeben wurde, beschloss das Trio andere Wege für seine Recherche einzuschlagen. Mit Laptops und Smartphones ausgerüstet, probierten sie zuerst, das Unternehmen von außen über das Internet anzugreifen, was jedoch nicht zum Erfolg führte. Daraufhin versuchten sie an unternehmensinterne Informationen zu kommen. Einer der Studenten besuchte die Firmenzentrale und bat darum die Toilette benutzen zu dürfen. Auf dem Weg dorthin kam er an zwei modernen, verglasten Besprechungszimmern vorbei und stellte fest, dass auf einem Flipchart die Zugangsdaten zum Unternehmens-WLAN festgehalten waren. Ein schnelles Foto mit dem Smartphone und schon waren die Türen für den nächsten Versuch geöffnet.

Von der Parkbank vor dem Firmengelände aus konnten sich die drei Laien-Hacker – die Fähigkeiten und Möglichkeiten der Studenten waren bei weitem nicht auf dem Niveau von echten Hackern – Zugriff auf das Produktionsnetzwerk verschaffen. Mit frei zugänglichen Software-Werkzeugen starteten sie einen sogenannten aktiven Netzwerkscan. Dabei wird durch verschiedene Methoden festgestellt, welche Geräte angeschlossen sind. Was die Studenten nicht bedachten ist die Tatsache, dass sich Struktur und Anforderungen von Netzwerken in der Produktion (OT) sehr von jenen in der Office-IT unterscheiden. Ein kritischer Faktor ist die Echtzeitkommunikation zwischen den Produktionsmaschinen. Der von den Studenten ausgelöste Netzwerk-Scan führte zu einem Stillstand der Produktionsanlage.

Was war passiert? Mehrere Sensoren konnten ihre Messwerte aufgrund einer erhöhten Netzwerklast nicht in Echtzeit an die Steuerung rückmelden. Diese interpretierte die Situation als kritisch für die an der Maschine arbeitenden Mitarbeiter und stoppte die Produktion. Der völlig überraschte Produktionsleiter versuchte den Fehler zu finden und zu beheben und die Produktionsanlage wieder zu starten, was aber nicht funktionierte, da der Netzwerk-Scan der Studenten noch immer aktiv war. Als diese ihre Datensammlung stoppten war es für den Keksproduzenten bereits zu spät. Teile der Produktionsanlage mussten vollständig zerlegt und gereinigt werden, da sich der Teig in den Spritzdüsen bereits verhärtet hatte. Der Gesamtschaden belief sich auf ungefähr 500.000 Euro.

Die Studenten konnten letztlich mit großem zeitlichen und finanziellen Aufwand ausgeforscht werden. [3.7]

3.2 SCHUTZ- UND GEGENMASSNAHMEN

BEWUSSTSEINSBILDUNG UND SCHULUNG DER MITARBEITERINNEN

Um Vorfälle wie diese auszuschließen, sollten in jedem Unternehmen folgende Fragen geklärt werden:

1. Sind sich alle Mitarbeiter der aktuellen Risiken und Bedrohungsszenarien bewusst?

2. Welche Auswirkungen hätte ein Stillstand von 1 Stunde/1 Tag/1 Woche?

3. Welche Schutzmaßnahmen sind bereits in der Fertigung/Produktion/Montage umgesetzt? Was gilt es zusätzlich zu tun oder zu verbessern?

4. Was muss im Krisenfall getan werden und wer hat dann welche Aufgaben zu verantworten?

VERWENDUNG SICHERER PASSWÖRTER

Mitunter führen schon einfache Maßnahmen zu einer erhöhten Sicherheit. Regeln zur Gestaltung von Passwörtern und deren Nutzung in unterschiedlichen Anwendungen sind dabei ein erster Schritt. Eine Grundregel lautet etwa, nie die gleiche Kombination von Mailadresse und Passwort in verschiedenen Anwendungen zu nutzen. Auf der Webseite https://haveibeenpwned.com/ ist zu finden, welche Zugangsdaten wie Mailadressen oder Passwörter bereits gehackt wurden und eventuell auch im Darknet gehandelt werden.

NOTIZEN

DOS- UND DDOS-ANGRIFFE

4

Ein Denial-of-Service-Angriff (DoS-Angriff) ist ein Versuch die IT- und Kommunikationsinfrastruktur eines Unternehmens durch Überlastung zu beeinträchtigen. Dabei werden Kommunikationseinrichtungen wie Webseiten, technische Geräte oder Server, welche eine aktive Verbindung mit dem Internet haben, überlastet. Dies geschieht durch eine sehr große Anzahl von gesendeten Datenpaketen oder Anfragen an das technische Gerät über die Kommunikationsverbindung. Durch die erzeugte Informationsflut kann die eigentliche Funktion nicht mehr ausgeführt werden. Ein solcher Funktionsausfall kann, je nach Intensität des Angriffs, Minuten, Stunden, aber auch Tage lang dauern.

Wird vom Angreifer ein sogenanntes Botnet verwendet, d.h. viele infizierte Computer im Internet die gleichzeitig diesen Datenverkehr generieren, spricht man von einem Distributed-Denial-of-Service-(DDoS) Angriff. Die Computer senden dann alle zum gleichen Zeitpunkt an eine bestimmte IP-Adresse ein Datenpacket oder eine Anfrage und erzeugen so die Überlastung. Wenn internetfähige Geräte durch den Angreifer aufgefordert werden ein Antwortdatenpacket an die Adresse eines Angriffsziels zu senden wird dies Distributed-Reflected-Denial-of-Service-(DRDoS) Angriff genannt.

Angegriffene Systeme ohne DDoS-Schutzmechanismen können ein solches übergroßes Verkehrsaufkommen nicht verarbeiten und somit bricht üblicherweise der normale Kommunikationsbetrieb zusammen. Betroffene Server oder Webseiten sind dann über das Internet nicht oder nur mehr eingeschränkt erreichbar.

Je mehr Computer in einem Botnet gleichzeitig verwendet werden, desto größer ist der erzeugte Datenverkehr und umso heftiger der Angriff. In der Vergangenheit wurden meist Netzwerksysteme wie Router, Firewalls oder Server durch eine Verkehrsüberlastung angegriffen. In letzter Zeit gewinnen auch Angriffe auf Applikations-Software immer mehr an Bedeutung. Mit zunehmender Wichtigkeit des Internets der Dinge (IoT) werden für DDoS-Angriffe auch Geräte missbraucht, die auf den ersten Blick harmlos wirken wie beispielsweise Internet-fähige Set-Top-Boxen, Überwachungskameras oder Sensoren eines Smart Homes. Diese Geräte werden oft mit Standard-Passwörtern ausgeliefert und ihre Firmware selten aktualisiert. Dies macht sie zu attraktiven Zielen für die automatisierte Übernahme in Botnets. Somit trägt der IoT Trend mittlerweile wesentlich zum Bedrohungspotential durch DDoS-Angriffe bei.

4.1 MOTIVATION FÜR DDOS-ANGRIFFE

Die Motivation einen DDoS-Angriff einzusetzen liegt überwiegend darin, einen höchstmöglichen wirtschaftlichen Schaden für den Angegriffenen zu erzeugen. Dies kann durch kriminelle Absichten erfolgen, wie z.B. die Erpressung von Lösegeld um den Angriff wieder zu beenden, aber auch Sabotageziele durch Konkurrenten, enttäuschte Kunden oder politisch motivierte Aktivisten können Gründe sein. DDos-Angriffe sind auch ein wesentliches Bedrohungspotential für die kritische Infrastruktur eines Landes, wie z.B. Energienetze, Kraftwerkseinrichtungen, öffentlicher Verkehr, Flughäfen und Behördeneinrichtungen und sind somit auch ein wichtiges Bedrohungsszenario für die Erhaltung der nationalen Sicherheit.

4.2 MÖGLICHE SCHÄDEN

Mögliche Schäden für ein Unternehmen reichen von umfangreichen wirtschaftlichen Verlusten durch Service- und Produktionsausfälle über Verkaufsentgang und Imageschäden am Markt bis hin zu unzufriedenen Kunden und Kundenverlust. Im Bereich der nationalen Sicherheit kann der Schaden durch die Beeinträchtigung kritischer Dienstleistungen auch eine gesamtstaatlich negative Auswirkung haben, wenn z.B. der öffentliche Transport nicht mehr aufrechterhalten werden kann.

4.3 SCHUTZ- UND GEGENMASSNAHMEN

Drei wichtige Maßnahmen sind zielführend, um vor DDoS-Angriffen geschützt zu sein:

- Einsatz von speziellen Geräten zur Überwachung des Datenverkehrs; d.h. spezielle Erkennungssensoren an den richtigen Stellen eines Netzwerkes welche mit einem modernen Security Information und Event Management System (SIEM)[3] verbunden sind. Dadurch kann ein Angriff frühzeitig erkannt werden.

- Einsatz von speziellen Netzgeräten am Eingang des Firmennetzes mit dahinterliegenden Netzinfrastrukturen, um im Angriffsfall den bösartigen Verkehr aus dem Internet herauszufiltern, umzuleiten und dadurch unschädlich zu machen (sogenannte Scrubbing Center).

- Vereinbarte Notfallprozesse mit dem Internetanbieter, der auch geeignete Möglichkeiten in seiner Netzinfrastruktur hat, um den Internetverkehr im Notfall rasch umleiten zu können.

4.4 BEISPIELE VON DDOS-ANGRIFFEN

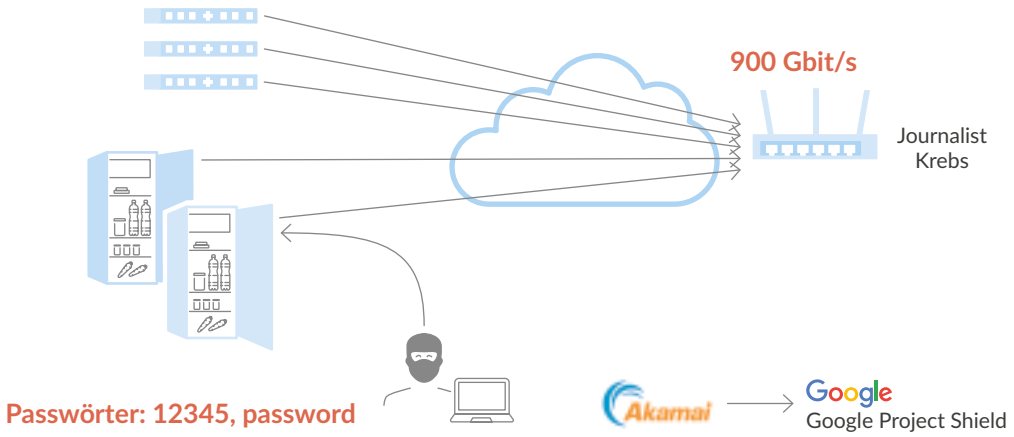
Ein DDoS-Angriff erfolgte 2016 auf den Netzbetreiber A1 [4.1]: „A1 wurde seit Samstag, 30. Jänner, wiederholt Opfer von sogenannten DDoS-Attacken (Distributed-Denial-of-Service). Bei dieser Art des Cyberangriffs wird die Netzinfrastruktur mit enorm vielen Datenpaketen, die über viele Länder verteilt abgeschickt werden, überlastet, um das Service des Internetzugangs zu stören. Dadurch war die Nutzung des mobilen Internets und einzelner mobiler Services teilweise nicht oder nur sehr verzögert möglich. Betroffen waren alle Kunden der Marken A1, bob, yesss! und Georg, die Internet über 2G, 3G und 4G am Smartphone, Tablet oder über ein Mobilfunkmodem nutzen."

Ein weiterer, sehr leistungsstarker DDoS-Angriff erfolgte 2016 mit dem sogenannten Mirai IoT Botnet-Angriff [5.2]. Dieser Angriff richtete sich gegen einen Journalisten, indem sein Online-Dienst gestört wurde. Bei diesem DDoS-Angriff wurden einige 10.000 nicht geschützte IoT-Geräte im Internet missbraucht, um einen Datenstrom mit einer Verkehrslast von 900 Gbit/s zu erzeugen. Dieser Angriff zeigte erstmals die Möglichkeit von DDoS-Angriffen durch die sehr große erzeugte Verkehrslast. Erst durch das Einschalten eines globalen Netzbetreibers wie Google konnte dieser massive Angriffsdatenverkehr wieder abgewendet werden, da nur Google derart leistungsfähige Netze weltweit in Betrieb hatte um die großen Verkehrsmengen in andere Netzbereiche umzulenken. Das Szenario des Mirai IoT DDoS-Angriffs ist in der Abbildung 4.1 skizziert.

[3] Security Information und Event Management Systeme (SIEM-Systeme) werden für die Überwachung von IT-Systemen eingesetzt. Sie alarmieren bei Angriffsversuchen auf Softwareanwendungen und Hardware.

Abbildung 4.1: MIRAI IOT BOTNET

System Vulnerabilities – „side channels“ Oktober 2016 „Mirai IoT Botnet“



Quellen: https://www.golem.de/news/nach-ddos-attacken-akamai-nimmt-sicherheitsforscher-krebs-vom-netz-1609-123419.html
https://www.golem.de/news/hilfe-von-google-brian-krebs-blog-ist-nach-ddos-angriff-wieder-erreichbar-1609-123453.html

GEFÄHRDUNG DURCH FERNWARTUNG

5

Unter Fernwartung versteht man den Zugriff von einem entfernten Standort über das Internet auf ein IT-System oder eine computergesteuerte Industrieanlage zu Wartungszwecken. Maschinen können aus der Ferne gepatcht, upgedatet, gesteuert oder administriert werden. Dadurch ist es nicht mehr notwendig, dass ein Spezialist persönlich zu der Maschine oder zu den IT-Systemen vor Ort kommt. Die nötigen Änderungen kann dieser bequem von seinem Arbeitsplatz aus erledigen, sogar wenn das System sich auf einem anderen Kontinent befindet. Durch Fernwartungsschnittstellen ist die oft teure Anreise eines Technikers nicht mehr notwendig, wodurch bei Störfällen schneller gewartet und kostengünstiger Wartungsprozesse durchgeführt werden können.

Das nachfolgende Beispiel erläutert Vorteile und Gefahren eines Zugriffs auf eine Produktionsanlage per Fernwartung:

Der Produktionsleiter einer mittelständischen österreichischen Fabrik arbeitet mit Industrieanlagen, die über das Internet mit einer Fernwartungsschnittstelle ausgestattet sind. Dadurch können seine Maschinen effizient und kostengünstig gewartet werden. Vor einigen Monaten wurde durch den Fernwartungszugriff ein Problem bei einer der Maschinen sehr einfach und schnell gelöst. Ein Spezialist des Anlagen-Herstellers hat über das Internet auf die Maschine zugegriffen und konnte somit die Ursache der Fehlermeldung schnell beheben. Ein kostspieliger Vorort-Einsatz, wie er früher notwendig war, konnte vermieden werden.

Dem Produktionsleiter war jedoch nicht bewusst, dass eine Schnittstelle für Fernwartungen durch entsprechende Maßnahmen abgesichert werden muss. Ein Krimineller hatte über die Fernwartungsschnittstelle Zugriff auf das System erlangt und Parameter der Steuerung verändert. Die Maschine begann schneller zu rotieren und somit zu überhitzen, was schließlich zu einem Totalausfall führte. Die Produktion stand für einige Tage still, der finanzielle Schaden war beträchtlich.

Was wie Fiktion klingen mag ist mittlerweile gängige Realität und bei der Umsetzung von Industrie 4.0-Projekten als reales Bedrohungsszenario zu beachten. Aus ExpertInnensicht ist der Einbruch über Fernwartungszugänge eine der Top-10-Bedrohungen im Bereich der Industrial Control Systems [5.1, 5.2]. Angriffe über Fernwartungszugänge erweisen sich insofern als gefährlich, als sie meist unbemerkt bleiben und auch schwierig zu erkennen sind.

5.1 SCHUTZ- UND GEGENMASSNAHMEN

Um Vorfälle wie diese auszuschließen, sollten in jedem Unternehmen folgende Fragen geklärt werden:

1. Welche physischen Zugänge und welche WLAN-Zugänge gibt es im Unternehmen und wie sind diese abgesichert?
2. Wie sieht die Trennung zwischen der Unternehmens-IT und dem Produktionsnetzwerk (OT) aus?
3. Gibt es klar kommunizierte Sicherheitsrichtlinien im Unternehmen und wie werden diese umgesetzt, auch gegenüber Gastzugängen?

Aufgrund der oben beschriebenen Problematiken kann eine Fernwartungsschnittstelle eine wesentliche Gefährdung für das Unternehmen darstellen. Mit verschiedenen organisatorischen und technischen Maßnahmen kann man allerdings ein IT-System absichern und Risiken maßgeblich minimieren:

ORGANISATORISCHE MASSNAHMEN

- Schulung des Personal bezüglich der Gefahren durch Industrie 4.0 Konzepte
- Festlegung von sicheren Prozessen für Fernwartungszugriffe
- Änderung von Standardpasswörtern oder Herstellerpasswörtern
- Dokumentation und Protokollierung der Zugriffe auf IT-Systeme zum Zweck der Nachvollziehbarkeit
- Überprüfung bzw. Auditierung durch externe Dienstleister

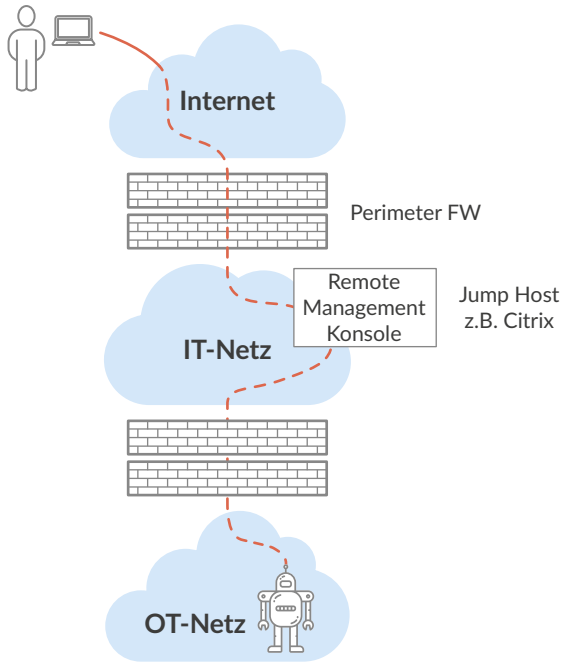
TECHNISCHE MASSNAHMEN

- Implementierung einer Netzwerksegmentierung in der IT und OT-Infrastruktur, um das Ausbreiten von Schadsoftware zu verhindern (siehe Abbildung 5.1). Eine hilfreiche Beschreibung dafür ist das Architekturmodell von Purdue[4].
- Freischalten von einzelnen Kommunikationssystemen (Ports) ausschließlich für bestimmte Zeiträume
- Zugriff auf Produktionsanlagen nur über besonders abgesicherte Netzwerke (sogenannte DMZ) ermöglichen
- Überprüfung der Geräte von WartungsmitarbeiterInnen auf Schadsoftware
- Eindeutige Identifikation von WartungsmitarbeiterInnen
- Sichere Verfahren zur eindeutigen Authentifizierung von WartungsmitarbeiterInnen durchführen, d.h. bei Login-Vorgängen durch WartungsmitarbeiterInnen spezielle Identifizierungsverfahren verwenden
- Sichere Datenübertragungen durch Verschlüsselung gewährleisten

Solche organisatorischen und technischen Maßnahmen sind in unterschiedlichen Standards definiert, wie z.B. ISO/IEC 27001[5], IEC 62443[6], NIST SP 800[7].

Da die Realisierung eines umfassenden Schutzes sehr aufwendig sein kann, ist es zielführend, auf Best Practice Erfahrungen von anderen Unternehmen zurückzugreifen.

Abbildung 5.1: BEISPIEL FÜR EINE NETZWERKSEGMENTIERUNG



[4] Das Purdue-Modell ist eine generische Architekturbeschreibung und Methode zur Absicherung für industrielle Steuerungsanlagen (ICS).

[5] ISO/IEC 27001 ist der zentrale Standard der ISO/IEC 27000-Familie, einer Serie von Standards zum Aufbau und Betrieb eines Information Security Management Systems (IMS). Diese Standards regeln im Wesentlichen grundlegende Geschäftsprozesse zur Realisierung von Informationssicherheit in Unternehmen, Behörden oder anderen Organisationen.

[6] IEC 62443 ist eine Serie von Standards für die Cyber-Sicherheit in industriellen Steuerungssystemen – Cybersecurity for Industrial Automation and Control Systems (IACS).

[7] Standards für Security und Privacy für Organisationen und Systeme der USA (US National Institute of Standards & Technology).

NOTIZEN

CLOUD SECURITY – KOMPROMIT-TIERUNG VON EXTRANET UND CLOUD-KOMPONENTEN

6

Industrieunternehmen nutzen heutzutage sowohl für ihre Produktionssysteme (Industrial Control Systems (ICS), als auch für andere Systeme (z.B. IoT-Geräte) Extranet- und Cloud-Komponenten zur Betriebsunterstützung, zur Fernwartung oder für die Einspielung von Software-Updates und Patches (IT-Virtualisierungsdienstleistungen). Diese Cloud-Dienstleistungen werden dabei üblicherweise bei externen IT-Dienstleistern betrieben (Infrastructure-as-a-Service oder Software-as-a-Service). Die eingesetzten Cloud-Lösungen bieten dem Industrie-Unternehmen besonders Kosteneinsparungen, da die notwendigen technische Systeme nicht selbst betrieben werden müssen, sowie bestimmtes IT-ExpertInnenwissen nicht mehr im eigenen Unternehmen aufgebaut werden muss.

Durch die Nutzung der Extranet- und Cloud-Komponenten ergeben sich allerdings spezifische Sicherheitsbedrohungen, welche von externen IT-Dienstleistern, aber auch von Industrieunternehmen zu beachten sind. In der Folge werden zwei dieser Bedrohungen beispielhaft beschrieben, sowie dargelegt, durch welche Gegenmaßnahmen die Bedrohungen behandelt werden können.

6.1 ABHÄNGIGKEIT DER PRODUKTION VON EINEM EXTRANET- UND CLOUD-DIENST

Geräte, die sich im Produktionsbetrieb mit einem Internetdienst des Herstellers verbinden, müssen normalerweise bei diesem Internetdienst des Herstellers registriert sein. Dadurch kann sich eine Abhängigkeit der Produktion von der Verfügbarkeit eines solchen Internetdienstes ergeben.

Ein typisches Beispiel für die Verwendung von Cloud-basierten Diensten im Zuge eines Produktionsprozesses und die mögliche IT-Sicherheitsproblematik ist im Folgenden dargestellt.

In unserem Szenario produziert ein Hersteller „smarte“ Geräte, die sich im Betrieb über ein Netzwerk des Kunden zu einem Internetdienst des Herstellers verbinden, um den Kunden ein besonderes Nutzungserlebnis zu bieten.

In einem bestimmten Schritt in der Produktion erhalten die Geräte eine eindeutige Identifikation, z.B. ein Geräte-Zertifikat im Zuge eines Konfigurationsprozesses. Mit dieser eindeutigen Identifikation können sich die Geräte später beim Internetdienst anmelden, um sich eindeutig zu authentifizieren. Für die Ausstellung der Identifikation, also der Gerätezertifikate, ist ebenfalls ein Internetdienst zuständig.

Die Geräte beinhalten ein Modul, einen Rechner mit Netzwerkschnittstelle(n). Sobald im Produktionsprozess die Firmware auf diesem Rechner installiert ist, generiert ein Programm ein Schlüsselpaar und verbindet sich zum Zertifikatsausstellungsdienst (CA – Certificate Authority). Die CA läuft bei einem externen Anbieter im Internet. Das heißt, die Geräte müssen sich von der Produktionslinie zu einem Dienst im Internet verbinden können. Sobald das Gerät sein Zertifikat von der CA erhalten und gespeichert hat, ist dieser Implementierungsschritt abgeschlossen.

Bis zum Erhalt des Zertifikats muss das Gerät aber jedenfalls warten. Somit sind Verfügbarkeit und Antwortzeit des CA-Dienstes unmittelbar relevant für die Effizienz der Produktion. Ein Ausfall der Verfügbarkeit bedeutet einen Stillstand der Produktion.

Im nächsten Schritt erhält das Produktionssystem das Gerätezertifikat vom Gerät und registriert das Gerät beim eigentlichen Internetdienst des Herstellers. Unser Hersteller hat dieses Verfahren gewählt, um den Zugang zu seinem Dienst auf echte Geräte zu beschränken.

Das Produktionssystem authentifiziert sich bei der Registrierungsschnittstelle des Internetdienstes und erhält die Berechtigung, neue Geräte (Clients) zu registrieren. Die Verfügbarkeit der Registrierungsschnittstelle des Internetdienstes ist also ebenfalls relevant für die Produktion.

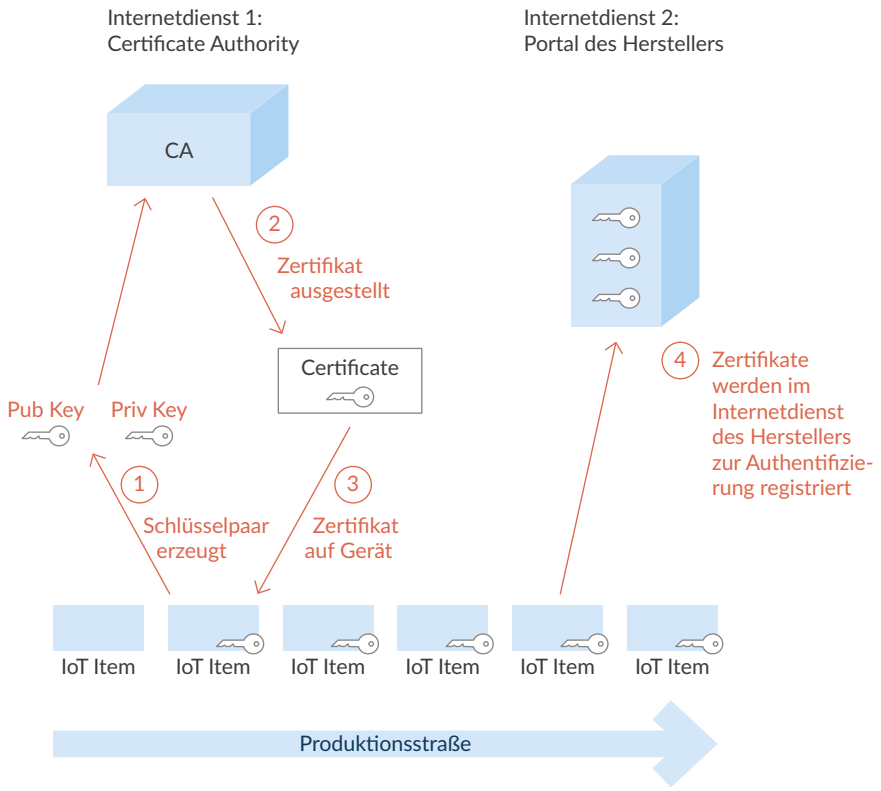
Um Sicherheitsvorfälle mit negativen Auswirkungen auf die Produktion zu verhindern sind folgende Maßnahmen notwendig:

- Die Authentizität des Produktionssystems muss gewährleistet sein, damit nur echte Geräte registriert werden können.

› Das Produktionsnetzwerk selbst muss strikt isoliert sein, sodass über die Authentifizierung der Geräte nicht von extern auf das Produktionsnetzwerk zugegriffen werden kann.

› Bei der Nutzung externer Dienste (z.B. Zertifikatsausstellungsdienst) im Zuge der Produktion muss darauf geachtet werden, dass die garantierte Verfügbarkeit des externen Dienstes mit den Anforderungen aus der Produktion übereinstimmt.

Abbildung 6.1: VERWENDUNG VON CLOUD-DIENSTEN FÜR EINE AUTHENTIFIZIERUNG VON IOT-GERÄTEN



6.2 UNZUREICHENDE MANDANTENTRENNUNG IN CLOUD-PLATTFORMEN

Industrieunternehmen können Teile ihrer für die Verwaltung oder (wenn auch seltener) für die Produktion benötigten IT-Komponenten auf Cloud-Plattformen von IT-Dienstleistern auslagern. Der IT-Dienstleister betreibt in diesem Fall die Systeme mehrerer Kunden gemeinsam auf derselben technologischen virtualisierten Cloud-Plattform.

Bei nicht-ordnungsgemäßer Trennung der Kunden (Mandanten) innerhalb dieser Cloud-Plattform durch den IT-Dienstleister sind unter Umständen Übergriffe zwischen den Netzen, Daten und Systemen verschiedener Mandanten möglich. Die Ursache dieser Übergriffs-Möglichkeit kann entweder eine Fehlplanung oder -konfiguration des IT-Dienstleisters sein, oder auch eine kritische Schwachstelle in der Virtualisierungstechnologie des Cloudanbieters.

Solche Systemschwächen können einerseits zur Spionage genutzt werden, z.B. von konkurrierenden Industrieunternehmen, welche denselben IT-Dienstleister nutzen. Andererseits besteht die Möglichkeit, dass ein gezielter externer Angreifer zunächst einen anderen Kunden des IT-Dienstleisters (z.B. über den Onlineshop des Kunden) ins Visier nimmt, und nach erfolgreicher Kompromittierung des ersten Kunden über die Übergriffsmöglichkeit auf sein Hauptziel, das Industrieunternehmen, zugreift.

Um dieser Bedrohung zu begegnen, müssen IT-Dienstleister darauf achten, dass ihre Cloud-Plattformen sicher und robust geplant und betrieben werden, um die Mandantentrennung zu gewährleisten. Die eingesetzten technischen Komponenten zur Plattform-Virtualisierung müssen auf aktuellem Stand gehalten werden, sowie kritische Sicherheitslücken rasch durch Updates geschlossen werden. Dabei muss der IT-Dienstleister auf die Wartbarkeit seiner Umgebung achten, sowie das Industrieunternehmen als Kunde bedenken, dass im Falle kritischer Sicherheitslücken der IT-Dienstleister in der Lage sein muss, seine Systeme zu patchen. Ein gut zwischen Dienstleister und Kunde abgestimmter Betriebs- und Patch-Plan inkl. Vereinbarung für Notfallpläne bei Sicherheitsvorfällen ist essentiell für die rasche Reaktion auf Sicherheitsbedrohungen im Extranet- und Cloud-Umfeld.

Um diesem Problembereich zu begegnen ist es wichtig, dass ein produzierendes Unternehmen einerseits Vertrauen in die Dienstleistung des Cloudanbieters hat – dies kann z.B. durch den Nachweis von Zertifizierungen oder durchgeführten Audits erfolgen.

VERLETZUNG DES DATENSCHUTZES DURCH IT-SICHERHEITS-LÜCKEN

7

7.1 MELDEPFLICHT BEI DATENSCHUTZVERLETZUNGEN

Das neue Datenschutzrecht (DSG und DSGVO) [7.1] beinhaltet eine verpflichtende Meldung bei Datenschutzvorfällen an die nationale Datenschutzbehörde und je nach Risiko für die Betroffenen auch an diese. Datenschutzrelevante Verletzungen (Datenpannen) können dabei schon durch den Verlust eines unverschlüsselten USB-Sticks mit Kundendaten oder mittels einer fehlgeleiteten E-Mail mit personenbezogenen Daten entstehen.

Was oft übersehen wird ist aber, dass auch durch einen Cyberangriff datenschutzrelevante Informationen betroffen sein können, was zu einem massiven Datenschutzproblem für das betroffene Unternehmen führen kann (Data Breach). Beispiele dafür sind das Bekanntwerden von Passwörtern oder auch Informationen über Kundendaten durch Cyberangriffe.

Wurden Datenpannen in der Vergangenheit in vielen Fällen nicht bekannt oder veröffentlicht, drohen nach der DSGVO beträchtliche Strafen bei der Nichtmeldung von solchen Problemen an die Behörde.

Neben einem möglichen Reputationsverlust bedeutet eine Datenpanne auch immer eine unmittelbare Mehrarbeit für das betroffene Unternehmen, um einerseits die Behebung der vorhandenen Schwachstellen durchzuführen und andererseits auch die Verminderung der negativen Auswirkungen sicherzustellen – durch technische und organisatorische Maßnahmen.

Wie im Artikel 33 DSGVO beschrieben, muss im Falle einer Verletzung personenbezogener Daten der Verantwortliche diese an die Aufsichtsbehörde melden und die Meldung muss *„eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen“* enthalten [7.2].

7.2 SCHUTZ- UND GEGENMASSNAHMEN

Im Kontext der unternehmensinternen Datenschutzmaßnahmen sind zwei wichtige Ansätze sehr hilfreich und wirken gleichzeitig sowohl für einen erhöhten Datenschutz als auch eine erhöhte Cyber-Sicherheit:

RISIKOMANAGEMENT

Zunehmend müssen sich auch KMUs mit den möglichen Risiken ihrer IT-Systeme beschäftigen. Dazu ist es notwendig, die unterschiedlichen Systeme zu evaluieren, mögliche Gefahrenquellen zu erkennen und technische sowie organisatorische Schutzmaßnahmen zu ergreifen. Dies wird so auch vom Datenschutzrecht gefordert.

Das Wissen unterschiedlicher Fachbereiche wie IT, Recht oder Human Resources muss dabei koordiniert und die Fachbereiche für ein gemeinsames Verständnis der Bedrohungsszenarien zusammengeführt werden. Denn die MitarbeiterInnen besitzen unterschiedliches Backgroundwissen, haben verschiedene Qualifikationen und Ausbildungen und verwenden in der Regel nicht die gleichen Fachbegriffe. Dies muss bei der Ausgestaltung von Maßnahmen berücksichtigt werden.

BEWUSSTSEINSBILDUNG UND SCHULUNG DER MITARBEITERINNEN ZUM DATENSCHUTZ

Vor allem auch KMUs müssen ihre MitarbeiterInnen in Bezug auf die geänderten technologischen Gefährdungssituationen sensibilisieren. Eine gesetzlich verpflichtende Verschwiegenheitserklärung unterschreiben zu lassen ist dabei nur ein erster Schritt (Datengeheimnis nach § 6 DSG). Es sind für die jeweiligen Aufgabengebiete und betrieblichen Systeme, sofern vorhanden unter Einbindung von Betriebsrat oder Personalvertretung, spezifische Schulungsmaßnahmen zu überlegen, umzusetzen und regelmäßig auf ihre Wirkung zu überprüfen.

CYBER-SECURITY HOTLINE 0800 888 133

8

Um den österreichischen kleinen und mittleren Unternehmen eine erste Hilfestellung und Unterstützung bei Cyber-Sicherheitsvorfällen anbieten zu können, hat die Wirtschaftskammer Österreich (WKO) ein österreichweites Dienstleistungsangebot implementiert. Klein- und Mittelbetriebe bekommen über eine österreichweite zentrale Stelle per Telefon als auch über das Web bei Cyber-Security Problemen eine Unterstützung.

8.1 SECURITY HOTLINE

Die Website für die Cyber-Security-Hotline lautet www.wko.at/cyber-security-hotline, bzw. auch WKO.at/cys oder www.cyber-security-hotline.at oder http://cys.at oder www.cys.at.

Die Cyber-Security-Hotline ist täglich von 0–24 Uhr und 7 Tage die Woche besetzt. Das Call Center führt eine Zufriedenheits- und Erfolgsmessung bei den Cyber-Crime-Opfern durch.

Wenn beispielsweise ein Unternehmen durch einen Ransomware-Trojaner lahmgelegt wurde, ruft das Unternehmen die Notfallnummer 0800 888 133 an und erhält vom Call Center Nothilfe im Sinne einer Erstversorgung. Sollte das Problem nicht sofort gelöst werden können, wird ein Second-Level mit IT-Security-Experten konsultiert. Hierfür wurde mit der WKO UBIT-ExpertsGroup IT-Security ein Team an hochspezialisierten IT-Sicherheitsexperten zusammengestellt. Das Call Center erstellt Tickets und gibt diese (i) an die Cyber-Security-Experten, (ii) an die Projektleitung und (iii) an die Servicecenter der Landeskammern weiter. Die Cyber-Security-Experten versuchen das Problem zu lösen. Die Erstberatung ist kostenlos, die Wiederherstellung von Daten wird firmenmäßig verrechnet.

ABWICKLUNG UND WORKFLOW

Im Call Center ist geschultes Personal beschäftigt und besitzt Kompetenzen im Notfallbereich. Für die Anrufe im Call Center wurde folgender Prozessablauf ausgearbeitet:

1. Prüfung, ob es sich um ein WKO-Mitglied handelt
2. Fälle, die kein Notfall sind, werden ausgeschieden
3. Telefonische Notversorgung (z.B. Anweisung zum kontrollierten Herunterfahren der Server)
4. FAQs und Checklisten für den Cyber-Crime-Notfall, die durch die WKO UBIT ExpertsGroup IT-Security ausgearbeitet wurden, werden kommuniziert
5. Zertifizierte Experten aus der UBIT-ExpertsGroup IT-Security Liste werden nach geografischer Nähe zugewiesen, Liste wird von UBIT-ExpertsGroup IT-Security gewartet
6. Das Call Center informiert den Anrufer, dass er von einem/einer IT-ExpertIn rückgerufen wird (8 bis 18 Uhr) und die Bearbeitung des Falles über dem Ausmaß eines Informationsgesprächs kostenpflichtig ist, wobei der/die IT-ExpertIn die Kosten selbst definiert. Der/Die IT-ExpertIn finalisiert den Fall und meldet dies an das Call Center.
7. Die Fälle werden als Tickets zur weiteren Bearbeitung dokumentiert.
8. In Zukunft soll dann auch vom WKO Call Center, nach Zustimmung des geschädigten Unternehmens, eine entsprechende Meldung an die Polizei als auch an das CERT.at erfolgen.
9. Und schließlich führt das WKO Call Center eine Zufriedenheits- und Erfolgsmessung durch.

Die Auswahl, Wartung und Ergänzung der IT-Security-Experten sowie die Geschäftszeiten erfolgt über die jeweiligen Bundeslandsprecher in Abstimmung mit DI (FH) Gerald Kortschak, BSc, CMC. Die Entscheidung, wie neue Berater auf die Liste kommen, obliegt grundsätzlich jedem Bundesland. Als Qualitätssicherheitsstandard gelten Industriezertifizierungen, hochkarätige Security Ausbildungen, wie beispielsweise der Incite Ausbildungskurs im Bereich Daten-

schutz und IT-Sicherheit [8.1]; d.h. die Experten müssen die Zertifizierung „Certified Data & IT-Security Expert“ absolvieren, um als Sicherheitsexperten in der Hotline agieren zu dürfen.

8.2 ANSPRECHPERSONEN IN DEN BUNDESLÄNDERN

Folgende WKO MitarbeiterInnen koordinieren in den Bundesländern (alphabetisch geordnet) die Cyber-Security-Hotline: (1) Burgenland: DI Karl Balla, Andreas Hafner, (2) Kärnten: Mag. Jutta Steinkellner, (3) Niederösterreich: Mag. Andreas Pircher, (4) Oberösterreich: Ing. Anton Fragner, MSc (5) Salzburg: Mag. Nina Gökler (6) Steiermark: Dr. Wolfgang Schinagl, (7) Tirol: Dr. Reinhard Helweg, (8) Vorarlberg: Sibylle Drexel, MA MSc und (9) Wien: Helmut Mondschein.

8.3 KOOPERATION MIT STAATLICHEN STELLEN UND ORGANISATIONEN/ VEREINEN

Die Cyber-Security-Hotline kooperiert mit dem Bundesministerium für Inneres (BMI) und dem Bundeskriminalamt (BKA). Als Kontakt- und Koordinationsstelle fungiert die WKÖ (Servicemanagement und IKT).

Mit dem Bundeskriminalamt (BKA) wurde vereinbart, dass bei Anzeigen von Cyber-Crime-Vorfällen in Unternehmen, die bei der örtlichen Polizei eingebracht werden müssen, auf die Cyber-Security-Hotline hingewiesen wird.

Des Weiteren erfolgt eine enge Zusammenarbeit mit den verschiedenen öffentlichen Einrichtungen in diesem Kontext:

- CSP Cyber Sicherheit Plattform (https://www.digitales.oesterreich.gv.at/cyber-sicherheit-plattform)
- CERT.at
- ACOnet-CERT (CERT des österreichischen Wissenschaftsnetzes)

8.4 STATISTIK

Im Zeitraum von 9.6.–31.12.2017 gingen 194 Anrufe bei der Cyber-Security-Hotline 0800 888 133 ein. Dabei wurden 17 Fälle (in weiterer Folge Tickets genannt) an die IT-Security Experten in den Bundesländern weitergereicht (geordnet nach Anzahl): (1) Oberösterreich: 8, (2) Tirol: 5, (3) Wien: 2, (4) Burgenland, Steiermark: 1.

Im Zeitraum von 1.1.–31.12.2018 gingen 432 Anrufe bei der Cyber-Security-Hotline 0800 888 133 ein. Dabei wurden 129 Tickets an die IT-Security Experten in den Bundesländern weitergereicht (geordnet nach Anzahl): (1) Oberösterreich: 33, (2) Wien: 32, (3) Niederösterreich: 20, (4) Steiermark: 16, (5) Tirol: 9, (6) Kärnten: 8, (7) Burgenland: 5, (8) Salzburg: 4, (9) Vorarlberg:2. 303 Fälle konnten direkt von den geschulten MitarbeiterInnen im Sinne eines Sofortservices abgeschlossen werden.

NOTIZEN

ANHANG

9

9.1 SCHADSOFTWARE

Im Frühjahr 2019 wurden bereits 900 Millionen verschiedene Schadprogramme (Malware-Samples) gezählt [9.1]. Die 60 führenden IT-Sicherheitsunternehmen in der Welt haben sich zur Anti-Malware Testing Standards Organization (AMTSO) zusammengeschlossen, um diese enorm wachsende Bedrohung gemeinsam zu bearbeiten und zu beherrschen (https://www.amtso.org/).

Im Folgenden sind beispielhaft wichtige Schadsoftware (Malware) Typen, welche weltweit hohe Bekanntheit erlangt haben, kurz beschrieben:

- **BlackEnergy** (Black Energy2 and Blackenergy3): Diese Schadsoftware wird üblicherweise als Teil von Anlagen in E-Mails von Word und PowerPoint Dokumenten verbreitet und wird aktiv, wenn ein Empfänger die Dokumente in solchen E-Mails öffnet. Die BlackEnergy Schadsoftware wurde ursprünglich 2007 entwickelt um über das Http Internetprotokoll DDoS-Angriffe durchführen zu können um IT-Systeme lahm zu legen. 2010 wurde eine Variante davon bekannt welche auch Angriffe in die IT-Systeme ermöglichte (Blackenergy2) und 2014 gab es eine Version (Blackenergy3) mit mehreren Funktionen und Möglichkeiten mit anderen Softwarebausteinen zu verbinden (https://en.wikipedia.org/wiki/BlackEnergy).

- **Mirai:** Durch die Mirai Schadsoftware, welche 2016 entdeckt wurde, können Geräte die mit dem Internet verbunden sind und mit dem Linux Betriebssystem arbeiten durch eine Fernsteuerung kontrolliert werden um dadurch große Datenmengen für DDoS-Angriffe zu erzeugen (https://en.wikipedia.org/wiki/Mirai_(malware)).

- **Stuxnet:** Stuxnet ist eine Schadsoftware welche 2010 entdeckt wurde. Stuxnet wurde für Cyberangriffe auf Steuerungssysteme von Industrieanlagen (SCADA Systeme) konzipiert welche mit dem Betriebssystem Windows funktionieren und hat mehrere sogenannte zero-day-exploits ausgenutzt (https://en.wikipedia.org/wiki/Stuxnet).

- **WannaCry:** Durch die WannaCry Schadsoftware konnten Windows-basierte IT-Systeme angegriffen werden indem diese Schwachstellen (exploits) im Betriebssystem Windows ausnutzten. Durch den Angriff wurden dann Daten verschlüsselt und die Opfer mit Lösegeld erpresst (deshalb wird diese Art von Schadsoftware auch Ransomware genannt) (https://en.wikipedia.org/wiki/WannaCry_ransomware_attack).

- **EMOTET** ist ein erfolgreiches Framework für Ransomware-Angriffe. Oft sind diese Angriffe auf den Gesundheitssektor ausgerichtet. In diesem Bereich wird der Umstand, dass immer eine unmittelbare Entscheidung notwendig ist, da Leben potentiell gefährdet ist, ausgenutzt. Siehe auch [9.2, 9.3]
  - https://www.srf.ch/news/wirtschaft/bedrohliche-cyberangriffe-wenn-der-operationssaal-stillsteht
  - https://www.heise.de/security/meldung/BSI-warnt-vor-gezielten-Ransomware-Angriffen-auf-Unternehmen-4406590.html

- **Regin** ist eine Malware, welche von westlichen Diensten wie NSA in Amerika und GCHQ in England verwendet werden, um Microsoft Windows basierte Computer anzugreifen (https://en.wikipedia.org/wiki/Regin).

- **Meltdown & Spectre** sind besondere Arten von Schadsoftware, welche bestimmte Schwächen (vulnerabilities) von modernen Micro-Prozessoren ausnutzen. Durch diese Schwächen können Daten, welche der Prozessor bearbeitet, unerlaubt ausgelesen und missbraucht werden. Da ein Prozessor im Kern eines Computer-Systems eingebettet ist, ist diese Schadsoftware eine besondere Bedrohung.

9.2 ABKÜRZUNGEN

AMTSO	Anti-Malware Testing Standards Organization
BMI	Bundesministerium für Inneres
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik aus Deutschland
CA	Certificate Authority
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CSP	Cyber Sicherheit Plattform
DoS	Distributed-Denial-of-Service
DRDoS	Distributed-Reflected-Denial-of-Service
FW	Firewall
HMI	Human-Machine-Interface
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologien
IoC	Indicator of Compromise
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
OT	Operational Technology
SIEM	Security Information und Event Management System
STB	Set-Top-Box
WKO	Wirtschaftskammer Österreich
WLAN	Wireless Local Access Network

9.3 GLOSSAR

- **AMTSO:** Die 60 führenden IT-Sicherheitsunternehmen in der Welt haben sich zur Anti-Malware Testing Standards Organization (AMTSO) zusammengeschlossen, um die enorm wachsende Bedrohung gemeinsam durch Schadsoftware zu bearbeiten und zu beherrschen (https://www.amtso.org/).
- **Botnet:** Mehrere infizierte Computer im Internet, welche für einen Cyberangriff vom Angreifer verwendet werden.
- **BSI:** Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de). Organisation in Deutschland welche Empfehlungen und auch Standards für IT- und Informationssicherheit herausgibt.
- **CEO-Fraud:** Angreifer geben sich als Teil des Unternehmens aus – z.B. als Geschäftsführer oder Finanzvorstand – aus und fordern von MitarbeiterInnen eine dringende Überweisung, beispielsweise durch eine gefälschte E-Mail an die Buchhaltung.
- **Computer Emergency Response Team (CERT):** Computersicherheits-Ereignis- und Reaktionsteam
- **Data breach:** Ein Sicherheitsvorfall bei dem ein Zugriff auf Daten möglich ist, ohne dafür eine Autorisierung zu haben.
- **Datenpannen:** Verletzung des Schutzes personenbezogener Daten
- **Denial-of-Service-(DoS) Angriff:** Erzeugung einer Verkehrsüberlast auf ein Gerät über das Internet
- **Distributed-Denial-of-Service-(DDoS) Angriff:** Wird eine große Zahl infizierter Computer gebündelt für einen DoS-Angriff eingesetzt, dann spricht man von einer Distributed-Denial-of-Service-Attacke (DDoS-Attacke). Die Computer senden dann alle zum gleichen Zeitpunkt an eine bestimmte IP-Adresse ein Datenpaket oder eine Anfrage und erzeugen so die Überlastung
- **Distributed-Reflected-Denial-of-Service-(DRDoS) Angriff:** Internetfähige Geräte werden dabei durch einen Angreifer aufgefordert ein Antwortdatenpaket an die Adresse eines Angriffsziels zu senden.
- **DMZ** Demilitarisierte Zone. Ein durch besondere technische Maßnahmen geschützter Netzbereich
- **DSG:** Datenschutzgesetz
- **DSGVO:** Datenschutz-Grundverordnung

- **Exploit:** Sicherheitslücken in technischen Systemen über welche Cyberangriffe möglich sind. Das Suchen nach solchen Systemschwachstellen ist das bestimmende Element für Kriminelle, organisierte Kriminalität und von Geheimdiensten.
- **Firewall (FW):** Technische Sicherheitsmaßnahme
- **Firmware:** Software, die im Gerät eingebettet ist
- **Forensik:** Suche in technischen Systemen um Schwachstellen zu identifizieren, bereits durchgeführte Angriffe zu erkennen oder auch um die Quelle des Angriffs zu identifizieren (Attribution).
- **ICS-CERT:** CERTS für Industrial Control Systems (ICS)
- **Indicators of Compromise (IoC):** Liste von Daten über Bedrohungen
- **Industrial Control Systems (ICS):** Steuerungssysteme für Industrieanlagen
- **Malware:** englische Bezeichnung für Schadsoftware; d.h. spezielle Softwaremodule mit denen in IT-Systeme eingedrungen werden kann um Schäden anzurichten.
- **Netzwerksegmentierung:** Vorgang, das Unternehmensnetz in einzelne Bereiche zu unterteilen, die nicht oder nur noch bedingt miteinander vernetzt sind, um für mehr IT-Sicherheit zu sorgen
- **Patch:** Software Updates
- **Ransomware:** Schadsoftware, damit kann dem/der ComputerinhaberIn der Zugriff auf Daten, deren Nutzung und das ganze Computersystem verhindert werden.
- **Office-IT:** IT für die üblichen Geschäftsprozesse
- **Operational-IT (OT):** IT für die verschiedenen Produktionsanlagen
- **Phishing:** Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen
- **Scrubbing Centre:** Zentralisierte „Datenreinigungsstationen", an denen Datenverkehr analysiert und schadhafte Daten entfernt werden.
- **Set-Top-Boxen (STB):** technische Geräte um Fernsehapparate an das Internet anzuschließen und interaktive TV Programmdienste zu realisieren
- **Shodan** (www.shodan.io): eine spezielle Suchmaschine um netzfähige Geräte mit Schwachstellen (Exploits) zu finden
- **Side Channels:** Nicht bedachte Funktionen von Software und IT-Systemen mit denen Schwachstellen entstehen oder mit denen Schutzmaßnahmen umgangen werden können.
- **SIEM-Systeme:** Security Information und Event Management (SIEM) Systeme werden für die Überwachung von IT-Systemen eingesetzt. Sie alarmieren bei Angriffsversuchen auf Softwareanwendungen und Hardware.
- **Social Engineering:** Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten.
- **System Vulnerabilities:** Schwachstellen von Software und IT-Systemen, welche ausgenutzt werden können um die Systeme in unerlaubter Weise zu beeinflussen.
- **Trojaner:** Malware, die sich oftmals als legitime Software ausgibt
- **WLAN Wireless Local Area Network (WLAN):** drahtloses lokales Netzwerk
- **Zero-day-exploits** sind Sicherheitslücken in technischen Systemen über welche Cyberangriffe möglich sind, welche aber dem Hersteller als auch den Benutzern der Systeme nicht bekannt sind, sondern die nur der Angreifer kennt. Das Suchen nach solchen Systemschwachstellen ist das bestimmende Element für Kriminelle, organisierte Kriminalität und von Geheimdiensten.

LITERATUR

10

Abschnitt 1

[1.1] F-Secure Deutschland, Threat Landscape Report zum zweiten Halbjahr 2018: Anzahl der Attacken ist um das Vierfache gewachsen, https://blog.f-secure.com/de/threat-landscape-report-h2-2018 (letzter Zugriff 1. August 2019).

Abschnitt 2

[2.1] McLaughlin, Stephen, et al. „The cybersecurity landscape in industrial control systems." Proceedings of the IEEE 104.5 (2016): 1039-1057.
[2.2] ICS-CERT. Year in review 2012. Technical report, Department of Homeland Security, 2013
[2.3] ICS-CERT. Year in review 2016. Technical report, Department of Homeland Security, 2017
[2.4] ICS-CERT. Year in review 2015. Technical report, Department of Homeland Security, 2016
[2.5] Lee, Robert M. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Technical Report, Dragos, Inc., 2017
[2.6] Obregon, Luciana. „Secure architecture for industrial control systems." SANS Institute InfoSec Reading Room (2015).
[2.7] Kobes, Pierre. Guideline Industrial Security: IEC 62443 is easy. VDE Verlag, 2017.

Abschnitt 3

[3.1] Republik Österreich, Bericht Cyber Sicherheit 2018, https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html (letzter Zugriff: 4. Mai 2019)
[3.2] Republik Österreich, Bericht Cyber Sicherheit 2017, https://www.digitales.oesterreich.gv.at/documents/22124/30428/Bericht-Cyber-Sicherheit+2017/9e3aa25d-2bf0-4c3c-841b-8c62f5dc8612 (letzter Zugriff: 4. Mai 2019).
[3.3] Der Standard, Cyberbetrug: Bisher 86 Millionen erbeutet, 21.6.2017, https://tinyurl.com/derStandard21Juni2017 (letzter Zugriff 4. Mai 2019)
[3.4] Kärnten ORF, Hotel zum vierten Mal von Hackern lahmgelegt, 22.1.2017, https://kaernten.orf.at/news/stories/2821290/ (letzter Zugriff 4. Mai 2019)
[3.5] BSI Analyse: das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus Deutschlanderstellt in regelmäßigen Abständen Analysen rund um das Thema Sicherheit (www.bsi.bund.de).
[3.6] Beispiel von Adrian Pinter, Siemens Aktiengesellschaft Österreich, 2019.
[3.7] Beispiel von Adrian Pinter, Siemens Aktiengesellschaft Österreich, 2019.

Abschnitt 4

[4.1] A1 Homepage, Cyber-Angriff auf A1 Infrastruktur, 2.2.2016, https://newsroom.a1.net/news-cyber-angriff-auf-a1-infrastruktur?id=59635&menueid=13054 (letzter Zugriff 4. Mai 2019)
[4.2] Josh Fruhlinger, The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, CSO, 9. März 2018. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (letzter Zugriff 4. Mai 2019)

Abschnitt 5

[5.1] Christina Fink, Erstellung eines Management-Models für Informationssicherheit im industriellen Internet, Masterarbeit, Fachhochschule Wiener Neustadt, 18.12.2017.
[5.2] Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2019, BSI-CS 005, Version 1.30, 01.01.2019.

Abschnitt 7

[7.1] WKO, EU-Datenschutz-Grundverordnung (DSGVO): Checkliste, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html (letzter Zugriff 4. Mai 2019)
[7.2] Art. 33 Abs. 3 lit. d DSGVO

Abschnitt 8

[8.1] Zertifizierung „Certified Data & IT Security, incite, Expert" https://www.incite.at/de/zertifizierungen/certified-data-it-security-expert/

Abschnitt 9

[9.1] AV-Test Sicherheitsreport, 2018/2019, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2018-2019.pdf
[9.2] https://www.srf.ch/news/wirtschaft/bedrohliche-cyber-angriffe-wenn-der-operationssaal-stillsteht und
[9.3] https://www.heise.de/security/meldung/BSI-warnt-vor-gezielten-Ransomware-Angriffen-auf-Unternehmen-4406590.html

WEITERFÜHRENDE LINKS

11

Links und Literatur zum Thema der EG Mitglieder ...

- CSP Cyber Sicherheit Plattform Österreich – https://www.digitales.oesterreich.gv.at/cyber-sicherheit-plattform)
- KSÖ Cyber Security – https://kuratorium-sicheres-oesterreich.at/allgemein/cyber-security/
- KSÖ Cyber-Risikomatrix – https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf
- Plattform Industrie 4.0, EG Security & Safety – https://plattformindustrie40.at/security-safety/
- Österreichischer Verband für Elektrotechnik, Gesellschaft für Informations- u. Kommunikationstechnik, Cyber Security – https://www.ove.at/ove-gesellschaften/git/aktivitaeten/cyber-security/
- AIT Austrian Institute of Technology, Center for Digital Safety & Security – https://www.ait.ac.at/en/about-the-ait/center/center-for-digital-safety-security/
- Seite zur Überprüfung, ob die eigene E-Mail-Adresse Teil von Daten-Leaks ist – https://haveibeenpwned.com/

AIT Austrian Institute of Technology:

- AIT Cyber Range – Trainings & Simulationsplattform: https://www.ait.ac.at/cyberrange/; https://cyberrange.at/
- AIT Safety & Security Co-Engineering: https://www.ait.ac.at/themen/dependable-systems-engineering/
- THREATGET – Cyber-Security-Management-System für den Fahrzeugsektor http://threatget.com/
- AECID – Intelligente Sicherheitstechnologie zur Anomalieerkennung in Netzwerken, basierend auf Artificial Intelligence (AI): https://www.ait.ac.at/aecid/; https://aecid.ait.ac.at//
- AIT Cyber Security Lösungs- und Technologieportfolio: https://www.ait.ac.at/fileadmin//mc/digital_safety_security/downloads/Factsheet_-_CyberSecurity_de.pdf
- Big Data Analytics for Network Traffic Monitoring and Analysis: https://bigdama.ait.ac.at/
- AIT Technologien rund um die Quantenverschlüsselung: https://www.ait.ac.at/en/research-fields/physical-layer-security/optical-quantum-technologies
- 5G – Reliable and Secure Wireless Technology for Industry 4.0 and Automotive: https://www.ait.ac.at/themen/physical-layer-security/
- GraphSense – Cross-Ledger Cryptocurrency Analytics Platform https://graphsense.info/, https://www.ait.ac.at/graphsense/

DANK

12

An diesem Leitfaden haben die Mitglieder der ExpertInnengruppe „Security & Safety“ der Plattform Industrie 4.0 Österreich mitgearbeitet.

Besonderer Dank gebührt dabei dem Redaktionsteam (in alphabetischer Reihenfolge):

Gregor Appeltauer, Industriellenvereinigung
Matthias Eckhart, SBA Research
Christina Fink, Kapsch BusinessCom AG
Nikolina Grgic, Plattform Industrie 4.0 Österreich
Martina Krucher, T-SYSTEMS Austria GesmbH
Helmut Leopold, AIT Austrian Institute of Technology
Adrian Pinter, Siemens AG Österreich
Thomas Riesenecker-Caba, Forschungs- und Beratungsstelle Arbeitswelt (FORBA)/AK Wien
Wolfgang Schinagl, WKO Steiermark
A Min Tjoa, Software Competence Center Hagenberg
Paul Trompisch, Plattform Industrie 4.0 Österreich

Folgende ExpertInnen wurden konsultativ eingebunden (in alphabetischer Reihenfolge):

Florian Achleitner, Fronius International GmbH
Peter Dorfinger, Salzburg Research
Mario Drobics, AIT Austrian Institute of Technology
Johannes Edler, FH OÖ
Tamer Elnahtawy,T-Systems
Wilfried Enzenhofer, UAR
Lukas Gerhold, Siemens
Franz Jantscher, voestalpine
Michael Lettner, BIZ UP
Bernhard Lueger, FH Technikum Wien
Viktorio Malisa, AUVA Allgemeine Unfallversicherungsanstalt
Thomas Mann, Kapsch BusinessCom AG
Siegmund Priglinger, pup consulting
Ingrid Schaumüller-Bichl, FH OÖ
Thomas Schober, voestalpine
Paul Smith, AIT Austrian Institute of Technology
Roland Sommer, Plattform Industrie 4.0 Österreich
Walter Wölfel, FH Technikum Wien

IMPRESSUM

Medieninhaber, Herausgeber und Hersteller:
Verein Industrie 4.0 Österreich – die Plattform für intelligente Produktion
Mariahilfer Straße 37–39, 1060 Wien
www.plattformindustrie40.at / office@plattformindustrie40.at

Projektleitung:
DI Helmut Leopold, AIT Austrian Institute of Technology, Leiter der ExpertInnengruppe „Security & Safety“
Nikolina Grgic, MSc, Verein Industrie 4.0 Österreich
DI Roland Sommer, MBA, Verein Industrie 4.0 Österreich

Design: confici® | Kreativbüro
Druck: Druckwerkstatt
Fotoquellen: Software Competence Center Hagenberg (9); AIT Austrian Institute of Technology (14); Kapsch BusinessCom AG (17); T-SYSTEMS Austria GesmbH (19); Shutterstock

Stand Juli 2019

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert. Für die Vollständigkeit und Richtigkeit des Inhaltes sowie für zwischenzeitliche Änderungen übernimmt der Herausgeber keine Gewähr.