ÖIAZ 165 WISSENSCHAFT & PRAXIS Dezember 2020

ÖSTERREICHISCHE
INGENIEUR-UND
ARCHITEKTEN-ZEITSCHRIFT

The JOURNAL of OIAV

Neue Technologien und Security in der Automatisierung

Dr. Lukas Gerhold – Siemens
Mag. Robert Schischka – CERT.at, NIC.at

Wie verändern digitale Technologien die industrielle Automatisierung?

Digitale Technologien finden schon seit mehreren Jahren Einzug in die Produktions- und Automatisierungswelt. Früher prägten – zum Teil proprietäre – Feldbusse die Automatisierung. Typische Anwendungen waren meist Insellösungen, deren Möglichkeiten zur Kommunikation beschränkt waren. Transparenz über die Gesamtsituation in der Produktion zu erlangen, war mühsam und mit erheblichem, teils manuellem Aufwand verbunden. In der Abbildung 1 sieht man anschaulich den Vergleich, auf welche Aspekte in einer digitalisierten Fertigung geachtet werden muss.

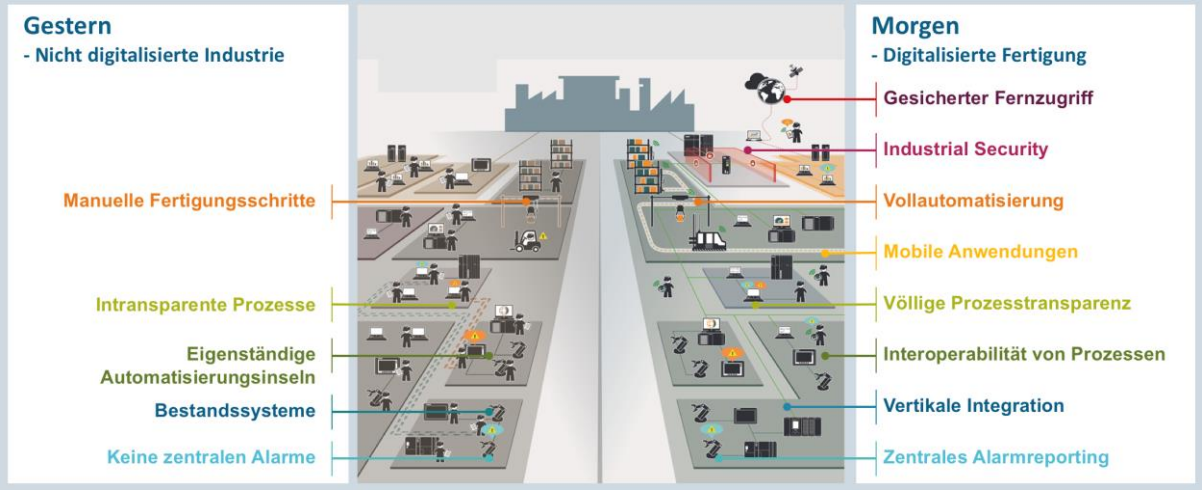

Abbildung 1: Automatisierung gestern – heute

Heutzutage finden standardisierte Netzwerktechnologien und Kommunikationsstandards (wie Ethernet, ProfiNet, OPC-UA, MQTT, etc. sowie Datenbanken ihre Anwendung in der Industrie. Diese Technologien ermöglichen bereits eine horizontale und vertikale Integration. Bei der *horizontalen* Integration liegt der Schwerpunkt auf der Kommunikation der Anlagen miteinander auf einer Ebene, – der Produktionsstätten untereinander (z.B. Lagermanagement, Auslastungsplanung) oder der digitalisierten Interaktion mit den Kunden und Lieferanten (Online-Verkauf, Austausch von Qualitätsdaten etc.). Die horizontale Integration gibt an, wie gut der Informationsfluss auf einer Ebene der Automatisierungspyramide funktioniert. Bei der *vertikalen* Integration sprechen wir über die Durchgängigkeit der

Informationen von der Feldebene und der Anlage bis hin zur Unternehmensebene und zurück. Die vertikale Integration gibt also an, wie gut der Informationsfluss zwischen den Ebenen der Automatisierungspyramide funktioniert. Abbildung 2 zeigt die Komplexität und die Herausforderungen, mit denen wir es derzeit bei der horizontalen und vertikalen Integration zu tun haben.

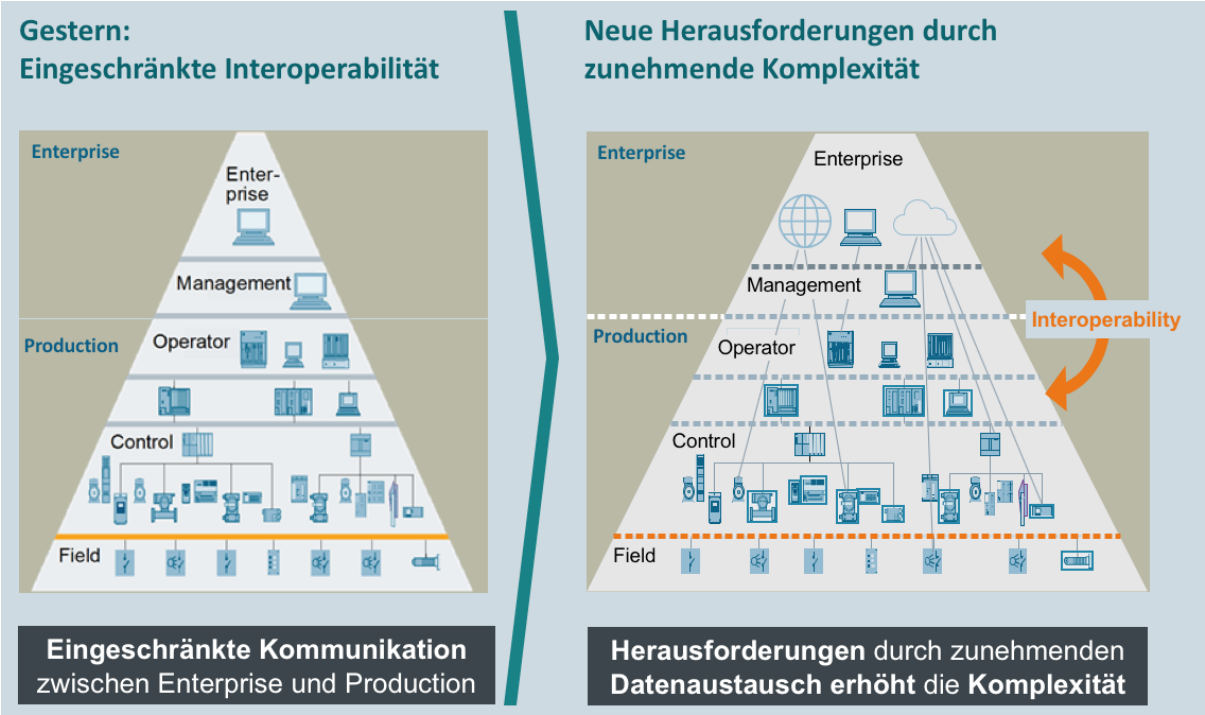

Abbildung 2: Horizontale und vertikale Integration

Die vertikale und horizontale Integration gelingt bereits vielen produzierenden Unternehmen; jedoch oft nur mit extrem hohem Aufwand für die Automatisierung und IT. Die Aufwände erwachsen durch Integration von Altsystemen in der Produktion und IT (z.B. ERP Systeme) sowie durch das laufende Integrieren von neuen oder adaptierten Anlagen.
Besonders das flexible Reagieren auf neue Marktanforderungen verlangt eine flexible Automatisierungslösung. Flexible Automatisierungslösungen bedeuten jedoch auch, dass die Datenstrukturen und Informationsstrukturen von und zur Anlage sich mit jeder Anpassung ändern. Das bedeutet wiederum selbst bei Verwendung von Standards eine Anpassung der Schnittstellen an der Anlage und den angebundenen (IT) Systemen oder den Verzicht auf die Gesamtheit der Daten, die in und für die Anlage zur Verfügung stehen.

Neue Technologien im Umfeld der Automatisierung

Neue Technologien in der Automatisierung versprechen eine deutliche Vereinfachung bei der Umsetzung der vertikalen und horizontalen Integration. Hierbei müssen diese Technologien, die unter anderem aus dem Umfeld der Automatisierung von Rechenzentren stammen, die speziellen Anforderungen in der Industrie erfüllen. Verfügbarkeits-, Vertraulichkeits- und Integritätsfunktionen wohnen diesen Technologien bereits inne. Jedoch müssen Technologien zur Verwendung im Automatisierungsumfeld zusätzlich Anforderungen wie Zuverlässigkeit, Safety und Wartbarkeit erfüllen. Daher ist eine sorgfältige Auswahl und genügend lange Phasen (Inkubationsphasen) bei der Einführung dieser Technologien essentiell.

Von welchen Technologien reden wir z.B.:

- Progressive Web Apps und Client- und Serverseitigen JavaScript Frameworks wie z.B. Node.js, Angular, uvm. oder
- Applikationsvirtualisierung wie z.B. Docker oder
- Cluster und Bigdata Technologien wie z.B. Kubernetes, Apache Kafka, Apache Hadoop oder
- Messaging und Streaming Frameworks wie MQTT, AMQP und Apache Flink,
- Technologien für Neuronale Netze und Mustererkennung wie z.B. OpenCV, Keras oder Tensorflow und

- Computer Chips für die Ausführung von Neuronalen Netzen wie Intel® Movidius™ Myriad™ X VPU und
- Höhere Programmiersprachen wie Python, JAVA, .NET Framework.

Die Liste der Technologien könnte nahezu beliebig fortgesetzt werden und die Auswahl zeigt lediglich einen Auszug aus den Projekten mit den derzeit höchsten Potentialen.
Die oben erwähnten Technologien finden Anwendung bei der Vor- und Nachverarbeitung von großen Datenmengen aus der Feldebene, bei Edge und IIOT Systemen, in HMIs, bei (On-Premises) Cloud Lösungen, generell im Management von Industrial Datacenters, Simulation und Digitalen Zwillingen oder beim Trainieren von neuronalen Netzen für komplexe Funktionen.

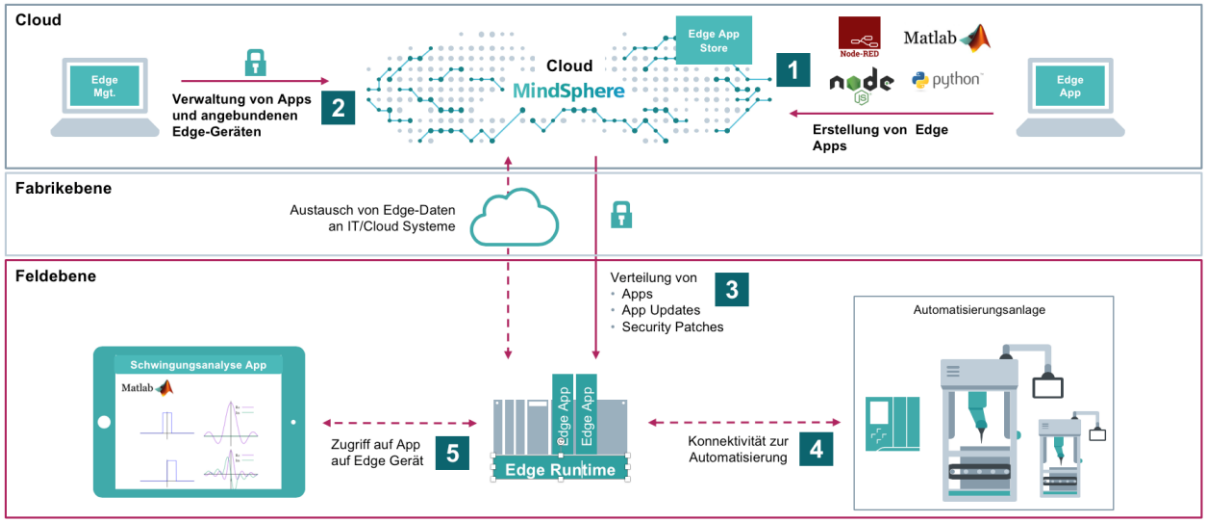

Abbildung 3: Industrial Edge Computing @ Siemens

In Abbildung 3 sieht man die Darstellung, wie SIMATIC Edge Computing die Datenverarbeitungsprozess in der Automatisierungswelt erleichtert. Im Schritt eins, in Abbildung 3 rechts oben, sieht man die „Erstellung von Edge Apps“. Das bedeutet, der Anwender des Edge Systems kann sich eine beliebige Applikation (App) z.B. in Python, C++, oder auch Node-Red selbst erstellen. Diese App ist dafür gedacht, im Feld auf einem Edge Gerät „deployed“, also eingesetzt und ausgeführt zu werden. Es gibt zusätzlich Apps, die man über einen Edge App Store herunterladen kann. Apps, die auf einem Edge Gerät laufen, können mit der Steuerung und Feldgeräten wie Sensoren kommunizieren und interagieren. Ein bidirektionaler Datenaustausch zwischen Edge Gerät und Automatisierung und Feldebene ist möglich. Edge Apps auf den Edge Geräten können ebenfalls miteinander kommunizieren. Hinter dem Schritt 2 „Verwaltung von Apps und angebundenen Edge-Geräten“ verbirgt sich der Edge Management Dienst. Das Edge Management ist ein zentraler Softwaredienst der On-Premise in einem (Industrial) Datacenter oder in der Cloud läuft und sämtliche Edge Geräte überwacht und die Software und die Apps für die Edge Geräte ausrollt, updated oder auch löscht. Somit erhält man die Kontrolle über die Edge Geräte und kann diese zentral warten und überwachen. Im Schritt 3 erfolgt das Deployment, also das Verteilen und Ausführen der Apps, Updates oder Security Patches auf den Edge Geräten. Schritt 4 „Konnektivität zur Automatisierung“ zeigt die bidirektionale Kommunikation mit der Automatisierungslösung. Beliebige Hersteller können über Standards wie OPC UA oder Message Broker wie MQTT oder direkt über Apps für die Kommunikation zur Automatisierungslösung angebunden werden. Der Schritt 5 „Zugriff auf App auf Edge Gerät“ symbolisiert die Offenheit des Systems, da jeder erdenkliche Zugriff, der vom Entwickler der App angedacht ist, möglich ist, wie z.B. Visualisierung über eine Web App, Web Services für die Erstellung von APIs und sogar low-level Socket Kommunikation ist realisierbar.

Typische Anwendungsfälle für Edge Computing sind die Aggregation und Aufbereitung von Informationen aus einer oder mehreren Automatisierungslösungen. Auf Basis dieser Informationen können z.B. komplexe Berechnungen durchgeführt werden, um die Automatisierungssteuerung zu entlasten bzw. um komplexe Zusammenhänge zwischen den Steuerungen zu berechnen und um diese wieder den Steuerungen bereitzustellen. Und natürlich können die Apps auf den Egde Geräten auch für die Weitergabe der Informationen an Cloud Systeme (Public Cloud oder Private Cloud) zum Einsatz kommen, dadurch können Datenbanken oder Big Data Systeme befüllt werden mit dem Ziel, den Gesamtüberblick über die im Feld befindlichen Systeme und Prozess zu erlangen. Anwendungen hierfür wären ein weltweites Asset Management, Update und Security Management der Automatisierungslösungen (generell aller

erfassten Geräte) im Feld, Predictive Maintenance, Tracken und Tracen von Anlagen und Anlagenteilen oder als Grundlage eines modernen Customer Care Services und Customer Managements. Auch weiterführende Datenauswertungen im Bereich mathematischer Statistik (Analytics) und das Trainieren von neuronalen Netzen (künstliche Intelligenz) sind auf Basis großer Datenbanken realisierbar.

Risiken der Digitalisierung und Maßnahmen zur Risikominderung

Da die horizontale und vertikale Integration (mit oder ohne neue Technologien) in jedem Fall einen erhöhten Einsatz von IT Technologien erfordert, erwachsen dadurch auch neue Risiken wie z.B.:

- der Verlust der Verfügbarkeit der Automatisierungslösung,
- der Verlust der Integrität der Funktionen der Automatisierungslösung oder der Daten,
- der Verlust der Vertraulichkeit der Informationen und der Kommunikation im Automatisierungsnetzwerk.

Die Ursachen für diese Risiken sind vielfältig, jedoch kann man sie grob in folgende drei Bereiche zusammenfassen:

1) Unzureichendes Wissen und mangelnde organisatorische Sicherheitsabläufe
2) Mangelnde Netzwerktrennung und Kommunikationssicherheit (Perimeter Schutz, Netzwerkzugriffsschutz, Netzwerküberwachung und Früherkennung von Angriffen, Fernwartung und Demilitarisierte Zonen)
3) Mangelnder Schutz der Systemintegrität und fehlende Endpoint Security (Systemhärtung, Punkt-zu-Punkt Verschlüsselung, Passwortschutz, Jumphost Konzepte, Security Policy Enforcement)

Maßnahmen wie der physische Schutz vor unbefugtem Zutritt zur Anlage sowie der Schutz des IT Netzwerks reichen heute bei Weitem nicht mehr aus, um sich vor Angriffen zu schützen. Daher wird von Siemens, um Gegenmaßnahmen zu den obigen Risiken zu entwickeln, die Einführung des Defense in Depth Konzepts empfohlen.

Abbildung 4: Defense in Depth @ Siemens Digital Industries

Abbildung 4 zeigt einen Überblick über das Defense in Depth Modell bei Siemens:

Anlagensicherheit, unter diesem Punkt summieren sich Maßnahmen wie z.B.:

1) Ausbildung im Bereich IT und Kommunikationstechnologien
2) Schwachstellen Management
3) Patch Management – wann und wie werden die Automatisierungssysteme (und verbundenen IT Systeme) aktuell gehalten und Security Patches eingespielt?
4) Physischer Zugangsschutz – wer darf die Schaltschränke, Technikräume, Serverräume öffnen und betreten und wie sind diese geschützt?
5) Notfall-Management – Was muss man tun, wenn doch einmal etwas passiert?

Netzwerksicherheit, hierunter befinden sich sämtliche Maßnahmen zur Absicherung von Kommunikations- und Netzwerktechnologien wie z.B.:

1) Netzwerktrennung – schaffen einer eigenen unabhängigen Netzwerkinfrastruktur (wichtigste Maßnahme zur Erhöhung der Verfügbarkeit der Anlage, aber auch der Wartbarkeit)
2) Zellschutz mit Industrie Firewalls oder direkt an der Steuerung über Kommunikationsprozessoren, die eine Firewall eingebaut haben
3) Monitoring, Netzwerküberwachung und Früherkennung von Angriffen

Systemintegrität und Endpoint Security umfasst alle Maßnahmen zur Sicherung der Funktionsweise der Applikationen und des gesamten Systems oder Anlage („das System soll das tun, was es tun soll"). Hierunter fallen Maßnahmen wie:

- Netzwerkzugriffsschutz, z.B. über IEEE 802.1x
- Systemhärtung
- Virenscanner und Virenschutz
- Know-how Protection, Copy Protection (z.B.: für Siemens S7 Steuerungen)
- Projektschutz (z.B.: im TIA Portal)
- HMI-Zugriffsschutz
- Kommunikationsintegrität – zertifikatsbasierte, verschlüsselte Verbindung zwischen den Endgeräten
- Anomalie-Erkennung und Intrusion Detection
- Zertifikatsbasierte, verschlüsselte Kommunikation z.B. über OPC UA

Allerdings gehören zu den Maßnahmen zur Minderung von Sicherheitsrisiken nicht alleine präventive Maßnahmen, sondern auch reaktive Maßnahmen.

Patch und Vulnerability Management

Eine Vulnerability oder zu deutsch Schwachstelle ist ein Fehler z.B. in Soft- oder Hardware, der von einem Angreifer ausgenutzt (exploit) werden kann. Es gibt bekannte Schwachstellen und unbekannte Schwachstellen – so genannte Zero-Day Vulnerabilities. Zero-Day Vulnerabilities sind jenen Personen unbekannt, deren Aufgabe es ist, die Software oder Hardware zu schützen und zu verbessern (z.B. Produkthersteller).
Jedoch viel wichtiger sind die bekannten Vulnerabilities – die unbedingt gemanagt werden müssen. Bekannte Vulnerabilities sind bereits öffentlich und können von jedem, auch von Personen mit schlechten Absichten eingesehen werden und ggf. ausgenutzt werden!
Siemens veröffentlicht bekannte Schwachstellen über das sogenannten Siemens ProductCERT:
https://new.siemens.com/global/de/produkte/services/cert.html
Zu jeder dort veröffentlichten Schwachstelle ist ein Link (siehe Advisory) zu einem Dokument, das die Schwachstelle beschreibt und auch die Vorgehensweise zur Minderung oder Behebung der akuten Bedrohung beinhaltet.
Ein proaktives Patch Management mit kontinuierlichem Überwachen der Vulnerabilities ist heutzutage eines der wirksamsten Mittel zur Abwehr von Security-Bedrohungen.

Eine Stelle, die bereits seit mehr als 10 Jahren präventiv und reaktiv im Bereich der IT-Sicherheit in Österreich arbeitet, ist CERT.at, das nationale Computer Emergency Response Team.

CERT.at – Informationsaustausch für Prävention und Reaktion

Seit 2008 verfügt Österreich über ein Computer Emergency Response Team (CERT). Dieses ist Teil der nic.at und hat sich zur Aufgabe gesetzt, das Internet in Österreich für alle sicherer zu machen. Mit dem Inkrafttreten des NIS Gesetzes (NISG) Ende 2018 gibt es nun auch einen klaren rechtlichen Rahmen für die Arbeit von CERT.at.
Seit seiner Gründung hat CERT.at bei zahlreichen Sicherheitsvorfällen von nationaler Relevanz als Informationsdrehscheibe fungiert, aber auch selbst Sicherheitsprobleme gefunden und aktiv an deren Behebung gearbeitet.

Information Sharing war von Beginn an eine der wichtigsten Aufgaben von CERT.at, denn allein das Sammeln derselben ist nicht ausreichend. Das Team bekommt Threat Intelligence von diversen nationalen und internationalen Quellen, bearbeitet die Daten und sendet Informationen an Betroffene in Österreich weiter. Dies geschieht zum größten Teil vollständig automatisiert und erfordert keine vorherige Anmeldung durch Betroffene.
Dabei ist dieser Vorgang aber keineswegs ein unidirektionaler Prozess: Staatliche und wissenschaftliche Institutionen sowie Unternehmen schicken häufig Beobachtungen von neuen Angriffen oder Taktiken Krimineller an CERT.at mit der Bitte, diese anonymisiert an andere potentiell Interessierte weiterzuleiten. Dass das funktioniert, liegt einerseits an der jahrelangen Arbeit zum Vertrauensaufbau durch das Team und andererseits daran, dass CERT.at nicht staatlich ist und deshalb, abgesehen von den Pflichtmeldungen nach dem NISG, keinerlei Informationspflichten gegenüber den Behörden hat.
Um einen direkten Austausch innerhalb einzelner Branchen (z.B. Energie, ISPs) zu fördern, hat CERT.at den **Austrian Trust Circle** (ATC) ins Leben gerufen. Diese Runden treffen sich regelmäßig, um sich in vertrauenswürdigen Rahmen über IT-Sicherheitsprobleme in ihren Bereichen auszutauschen und mögliche Gegenmaßnahmen zu besprechen.
Die Grundeinstellung „Sharing is caring" ist in diesem Zusammenhang unabdingbar, denn sie führt dazu, dass alle sicherer werden, egal wer eine neue Bedrohung zuerst gesehen hat.
Meldungen an CERT.at sind seit Inkrafttreten des NISG für die darin definierten Betreiber wesentlicher Dienste verpflichtend, wenn IT-Sicherheitsvorfälle eine gewisse Dimension erreichen. Wer als Betreiber eines wesentlichen Dienstes gilt, wird per Bescheid durch das Bundeskanzleramt bekanntgegeben. Eine solche Meldung muss über das NIS-Portal erfolgen, welches unter https://nis.cert.at zu finden ist.
Durch die Möglichkeit der Freiwilligenmeldung nach NISG kann man CERT.at auch im Sinne des oben genannten Information Sharing Vorfälle bekanntmachen und – wie auch bei einer Pflichtmeldung – Unterstützung anfragen.
Zusätzlich zu den Pflicht- und Freiwilligenmeldungen ist eine Meldung per E-Mail an reports@cert.at oder per Telefon an +43 1 5056416 78 jederzeit möglich.

Als Unternehmen profitieren Sie von CERT.at gleich mehrfach:

- Sie erhalten Reports zu Schwachstellen, infizierten Geräten und
- über die Mailingliste „Warnings" erhalten Sie Informationen über akute Bedrohungen, die sofortige Aufmerksamkeit erfordern.
- Auf der Mailingliste „Daily" finden Sie täglich eine Zusammenfassung der aktuell wichtigsten Themen und Entwicklungen im Bereich der IT-Sicherheit.
- Auf der MISP („Malware Information Sharing Platform") Instanz von CERT.at finden Sie „Indicators of Compromise" (IoCs) zu zahlreicher Schadsoftware, die von anderen aus der Community geteilt wurden und können andererseits Ihre Erkenntnisse dort zur Verfügung stellen.
- Bei den von CERT.at organisierten Treffen des ATC können Sie sich mit Unternehmen aus Ihrer Branche über spezifisch für Sie relevante Entwicklungen in der IT-Security austauschen.

SIRF, das Security Incident Response Framework, ist ein Toolkit, das im Austrian Energy CERT (AEC) in Kooperation mit CERT.at entwickelt wird. Das Ziel ist es, eine Plattform zu haben, die auch von „Gelegenheits-Incident-Respondern" verwendet werden kann. Dabei handelt es sich um Personen, die zwar für die Bearbeitung von Sicherheitsvorfällen verantwortlich sind, diese aber nur einen Teilbereich ihrer Gesamtaufgaben darstellen. Diese Situation hat oft zur Folge, dass sich einerseits keine Routine bei den Verantwortlichen einstellen kann, andererseits jedoch kaum Zeit für Trainings und Übungen vorhanden ist.
SIRF setzt sich genau hier zur Aufgabe, Fehler und Frustration zu vermeiden, indem es alle notwendigen Tools inklusive deren Dokumentation kombiniert. Die eingesetzten Tools sind größtenteils Open Source oder kostenlos verfügbar.
Außerdem soll SIRF Ablaufpläne und Templates erhalten, die helfen sollen, den Ablauf besser zu strukturieren. Darüber hinaus wird auch die Vorbereitung auf Vorfälle thematisiert, indem beispielsweise Tipps gegeben werden, welche Daten (Logs etc.) im Ernstfall üblicherweise benötigt werden.