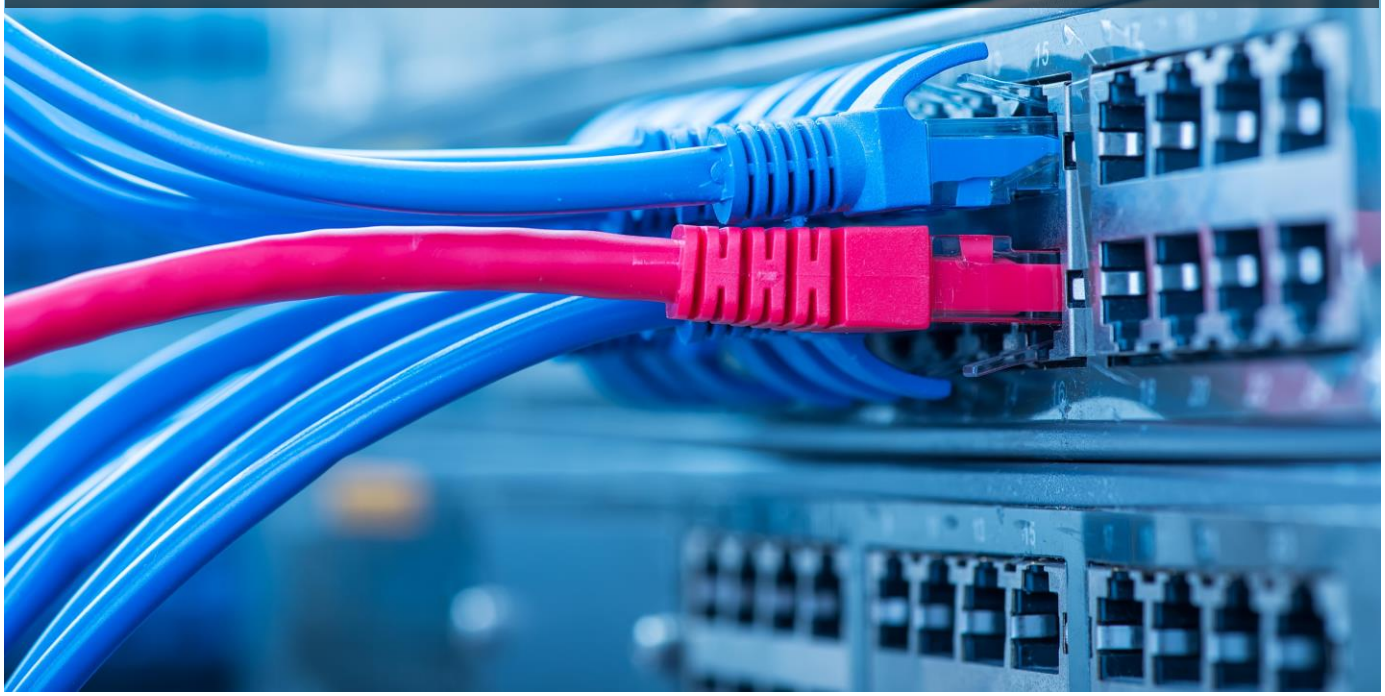
satw it's all about technology

Industrielle Kontrollsysteme sicherer machen



1 Management Summary

Kritische Infrastrukturen und deren Gesundheitszustand: In der Schweiz dürfen wir stolz sein auf gut funktionierende und robuste Infrastrukturen, die bis jetzt in den meisten Fällen auf sehr hohem Niveau stabil und sicher funktionieren. In den vergangenen Jahren wurden jedoch Ausbau, Betrieb und Nutzung zu minimalen Kosten optimiert, was in den Infrastrukturen und deren Weiterentwicklungen Spuren hinterlassen hat. Diese Spuren entstanden aufgrund des ständig zunehmenden Kostendrucks auf alle Service-Provider und führten zum Abbau von Redundanzen. Das Resultat ist ein degradierter Gesundheitszustand[1] der Infrastrukturen, welcher als Indikator für die Robustheit gegen Störungen dient. Zusätzlich führen Digitalisierung und Vernetzung zu neuen Verletzlichkeiten:

- **Digitalisierung zur Optimierung:** Die Infrastrukturen werden seit kurzem mit Methoden der Digitalisierung überwacht und optimiert. Dies ermöglicht eine höhere Auslastung, führt aufgrund ökonomischer Überlegungen auch zum Abbau von Reserven und Redundanzen.
- **Hyper-Konnektivität:** Die Digitalisierung erlaubt Verbindungen von bisher getrennten Infrastrukturen bis hin zur Hyper-Konnektivität (alles mit allem zu vernetzen). So verschmelzen durch die zunehmende Vernetzung auch die ehemals getrennten Bereiche der klassischen IT und der Operational Technology (OT). Die entstehenden Abhängigkeiten bringen neue Sicherheitsrisiken mit sich.
- **Vernetzung und Verletzlichkeit:** Die zunehmende digitale Vernetzung erhöht die Angriffsfläche der Informations- und Kommunikationstechnik (IKT). Zwar wurden die Schnittstellen meistens mit IT-Sicherheit ausgestattet, jedoch nicht genügend, um alle neuen Verletzlichkeiten zu kompensieren. Viele Expertinnen und Experten[2] befürchten deshalb, aufgrund des Kostendrucks und der weltweit zunehmenden Cyber-Bedrohungen, ein dominoartiges Kollabieren einer oder mehrerer Infrastrukturen. Das Resultat könnten schmerzhafte Erfahrungen mit länger andauernden Ausfällen sein.

Erneuerung und Wartung in IKT und OT: Zu einer Schwächung des Gesundheitszustandes der Infrastruktur trägt zudem bei, dass die OT-Ingenieure der Thematik der Cyber-Risiken oft zu wenig Beachtung schenken. Insbesondere liegt die Herausforderung in den Erneuerungs- und Wartungszyklen, die sich bei IKT und OT stark unterscheiden. In der OT betragen die Erneuerungszyklen 25 bis 40 Jahre, während sie im Bereich der IKT drei bis fünf Jahre umfassen. Die Wartungszyklen dauern in der OT oftmals Jahre, während sich diese in der IKT im Rahmen von Stunden bis Wochen erstrecken. Deshalb sind sich die OT-Ingenieure gewohnt, dass eine Infrastruktur jahrelang ohne wesentlichen Unterhalt betrieben werden kann und das Verständnis für Updates, die für IKT täglich oder wöchentlich erfolgen müssen, ist neu und schwierig zu vermitteln. Gegenseitiges Verständnis zwischen der OT- und IKT-Gemeinschaft muss deshalb bewusst erarbeitet werden, da die Natur und die Kurzlebigkeit der IKT den bisherigen Erfahrungen der OT widerspricht.

Kritische Infrastrukturen, ICS und Sicherheit: Kritische Infrastrukturen (z.B. Telekommunikation, Energie, Verkehr) sind für das Funktionieren unserer Gesellschaft, der Wirtschaft und des Staates essenziell, weshalb deren Schutz vor Cyber-Bedrohungen prioritär behandelt werden muss. Innerhalb der kritischen Infrastrukturen spielen Industrial Control Systems (ICS), eine besonders wichtige Rolle und deren Funktionsfähigkeit muss zwingen aufrechterhalten werden. Aufgrund zweier technischer Eigenschaften der ICS – Echtzeitfähigkeit und knapp bemessene IT-Ressourcen – ist es jedoch schwierig, diese zu schützen.

Sieben Empfehlungen zur ICS-Sicherheit: Die Empfehlungen des vorliegenden Berichts zeigen mögliche Vorgehensweisen zur Sicherung der ICS in kritischen Infrastrukturen und entsprechen weitgehend den weltweiten ICS-Sicherungsbemühungen. Ex-

[1] https://www.enisa.europa.eu/publications/maturity-levels/at_download/fullReport
[2] Die Bezeichnung «Experten» bezieht sich im folgenden Bericht auf die Autoren, sofern keine weiteren Erläuterungen angebracht sind.

pertinnen und Experten der SATW, aus der Industrie sowie von Bundesbehörden haben diese Empfehlungen gemeinsam erarbeitet, welche die wichtigsten Eckpfeiler für die Erhöhung der Robustheit und Sicherheit von ICS darstellen. Die sieben Empfehlungen sind:

- Konsequente Analyse der Gesamtsysteme, Abhängigkeiten und Risiken
- Neue Funktionalitäten (und deren Einbindung in bestehende Systeme) analysieren
- Robustheit und Resilienz stärken
- Security by Design
- Schulung der Mitarbeitenden
- Aufbau eines Schweizer ICS Computer Emergency Response Team (ICS CERT)
- Internationale Vernetzung und Informationsaustausch

ICS-Sicherheit und Entscheidungsträger: Die angesprochenen Verantwortlichen aus Politik, Wirtschaft und Verwaltung zusammen mit den Infrastrukturbetreibern entscheiden darüber, ob die Sicherheit entsprechend der steigenden Bedrohungen jetzt erhöht wird oder ob der Schutzgrad erst reaktiv, d.h. nach schmerzlichen Erfahrungen mit IKT-Sicherheitsvorfällen, ausgebaut wird. Die Autoren des vorliegenden Berichts sind sich einig: Aufgrund der Zunahme der Bedrohungen ist jetzt ein rasches Handeln angezeigt.

2 Einleitung

Cyber-Bedrohungen nehmen stetig zu. Bitkom[3] berechnete im Jahr 2015 den gesamten Schaden, der durch digitale Angriffe für die deutsche Wirtschaft entstand, auf 51 Milliarden Euro. Rechnet man diesen Betrag aufgrund der Einwohnerzahl auf die Schweiz um, so resultiert daraus eine geschätzte jährliche Schadenssumme von rund 5 Milliarden Schweizer Franken – das entspricht in etwa einer Verdreifachung des finanziellen Schadens im Vergleich zu 2012. MacAfee[4] schätzt weltweit die Schadenssumme auf rund 0,5 bis 1 Prozent der Wirtschaftsleistung, was für die Schweiz eine ähnliche Grössenordnung der Schäden ergibt. Zu den Angriffszielen gehören auch die IKT der kritischen Infrastrukturen. Für diese gibt es heute nur teilweise verbindliche Richtlinien, wie sie sich vor Cyber-Bedrohungen schützen sollten oder müssten (z.B.im Nuklearsektor die Regelungen des Eidgenössischen Nuklearsicherheitsinspektorats ENSI)[5]. Viele Betreiber sind sich der möglichen Cyber-Bedrohungen noch zu wenig und vor allem nicht auf allen Führungsebenen bewusst oder scheuen grosse Investitionen auf diesem Gebiet. Budgets für Massnahmen werden deshalb, auch bei ausgewiesenen Risiken, oft nur zögerlich oder gar nicht freigegeben.

Die unternehmerische Führung handelt grundsätzlich nach betriebswirtschaftlichen Grundsätzen. Daher werden primär die unternehmerischen Risiken adressiert. Bei kritischen Infrastrukturen gilt es aber, auch volkswirtschaftliche Risiken zu beachten. Nach Liberalisierungs- und Privatisierungsprozessen ist jedoch unklar, wer die Verantwortung für diese volkswirtschaftlichen Risiken trägt. Heute wird in dieser unklaren Situation auf Gespräche zwischen dem Staat und Vertretern der kritischen Infrastrukturen gesetzt, die durch Einsicht und Verständnis die komplexe Situation schrittweise einer Lösung zuführen. Der Vorteil dieses Vorgehens liegt darin, dass keine expliziten und hohen Kosten anfallen, weder beim Staat noch beim Betreiber, weil jeder Akteur die Kosten selbst trägt. Jedoch ist dieses Vorgehen langsam und erzeugt nur moderaten Druck, um die Cyber-Sicherheit rasch und massiv zu erhöhen.

Bislang sind in der Schweiz keine grösseren Probleme im Bereich der industriellen Kontrollsysteme (Industrial Control Systems, ICS, siehe Glossar) bekannt geworden, denn es gab nur wenige und eher unbedeutende Vorfälle. Die Autoren des vorliegenden Berichts sehen jedoch eine schnelle Zunahme kritischer Cyber-Bedrohungen mit stark ansteigendem Schadenspotenzial und sind besorgt, dass es in naher Zukunft schmerzhafte und lange andauernde Vorfälle geben könnte[6]. Bisherige Fälle, wie die Malware Stuxnet und Industroyer[7], die im Dezember 2016 als erste öffentlich bekannt Malware für Energienetze das Stromnetz der Ukraine lahmlegten, haben Sicherheitsdefizite deutlich aufgezeigt. Der Wunsch nach Klärung der Verantwortlichkeiten wird deshalb immer dringender, bedingt jedoch die Zuweisung der Kostenträger. Genau davor drückten sich bisher die Entscheidungsträger, weil unangenehm hohe Investitionen und Restriktionen in der Freiheit der digitalen Vernetzung zu erwarten sind.

2.1 Weshalb dieser Bericht?

ICS sind aufgrund ihrer Bedeutung für die Steuerung und Überwachung der Produktion sowie für die Bereitstellung von Dienstleistungen in verschiedenen Sektoren besonders kritische Komponenten der Infrastruktur: Deren Ausfall kann weitreichende Konsequenzen haben. National gibt es bereits einige Dokumentationen, die Betreibern von kritischen Infrastrukturen im Umgang mit Cyber-Risiken als Leitfaden dienen. Im speziellen Fall der ICS sind in der Schweiz grundlegende Empfehlungen vorhanden und frei verfügbar[8]. Die vorhandenen Empfehlungen werden von den adressierten Stellen jedoch (noch) nicht im notwendigen Masse umgesetzt. Es ist daher essenziell, dass bereits bestehende und die ergänzenden Empfehlungen in diesem Bericht von möglichst allen ICS-Anwendern zur Kenntnis genommen und vor allem umgesetzt werden.

Generelle Standards und Empfehlungen für allgemeine IT-Systeme sind genügend vorhanden. Deshalb befasst sich dieser Bericht mit Cyber-Bedrohungen ausschliesslich bezüglich ICS, da in diesem Bereich die Empfehlungen noch

[3] https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html
[4] https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
[5] Allgemeine Rahmenwerke lassen viel Interpretationsspielraum offen und decken die notwendigen Anforderungen nur teilweise ab.
[6] Vergleiche beispielsweise Halbjahresbericht MELANI, 2016/II
[7] https://en.wikipedia.org/wiki/Industroyer
[8] Beispielsweise der Leitfaden von MELANI «Massnahmen zum Schutz industrieller Kontrollsysteme»

zu wenig bekannt und konsolidiert sind. Der vorliegende Bericht unterstützt die nationalen Bemühungen zum Schutz von ICS in diesem Bereich und steht im Einklang mit diesen. Ausserdem gilt es zu beachten, dass von allen IT- und ICS- Komponenten einer kritischen Infrastruktur nur eine Untermenge als kritisch bewertet wird[9]. Nur diese kritische Untermenge muss diesen Empfehlungen folgen. Eine Risikoanalyse für die kritischen Infrastrukturen ist zwingend (gemäss nationaler Vorgabe) und identifiziert die zu schützenden Objekte der kritischen Infrastruktur (zu schützende Untermenge der kritischen Infrastruktur).

2.2 Methodisches Vorgehen

Auf Initiative der SATW haben sich Verantwortungsträger aus der Bundesverwaltung und Experten in spezifischen Bereichen zusammengeschlossen, um das Umfeld zu analysieren und gemeinsam Empfehlungen für den Schutz von ICS in kritischen Infrastrukturen zu erarbeiten. Dazu wurden Hearings durchgeführt, bei denen kompetente Vertreter der Sektoren Energie, Transport und Logistik, Gesundheit, Pharmazeutik und Chemie sowie Kommunikation und Finanzen einbezogen wurden. Hauptziel der interdisziplinären Zusammensetzung war es, die bei Behörden und Betreibern kritischer Infrastrukturen bestehenden Bestrebungen zum besseren Schutz von ICS zu verstärken und konkrete Handlungen anzuregen. Basierend auf den Hearings wurden Empfehlungen erarbeitet, die in diesem Dokument beschrieben werden.

2.3 Adressaten und Anwendung

Dieser Bericht bildet mit seinen Empfehlungen die Essenz der wichtigsten Eckdaten zur Sicherheit von ICS. Die Beschreibung soll trotz des Schwierigkeitsgrades der fortgeschrittenen Technik auch von der Allgemeinheit nachvollzogen werden können und ist deshalb in einfacher Sprache abgefasst. Auf höherer Management- und Entscheidungsebene bei Betreibern kritischer Infrastrukturen und in der nationalen Politik sollen die Empfehlungen eine lösungsorientierte Diskussion über die Sicherheit von ICS anregen.
Ein rasches Handeln ist angezeigt, da die Dichte und die Professionalität der Cyber-Angriffe keinen Zweifel darüber lassen, ob kritische Infrastrukturen in der Schweiz angegriffen werden, sondern lediglich wann und mit welcher Heftigkeit. Wesentlich ist, dass sich die Schweiz auf hohem Niveau gegen die Gefahren aus dem Internet schützt und auf Bedrohungen vorbereitet ist, um im Falle eines Angriffs möglichst rasch wieder über funktionierende Infrastrukturen zu verfügen.
Die SATW erwartet von der Politik das sorgfältige Studium der Empfehlungen und das lösungsorientierte Durchsetzen in allen kritischen Anwendungen von ICS-Komponenten bei kritischen Infrastrukturen. Von den Verantwortlichen in Verwaltung und Wirtschaft erwartet die SATW das Einfordern der rechtzeitigen und risikobasierten Implementation von ICS-Sicherheitsmassnahmen in den adressierten Bereichen.

2.4 Kapitelstruktur

Kapitel 3 zeigt die Positionierung der Empfehlungen im aktuellen Umfeld. Die Empfehlungen für sichere ICS (Kapitel 4) bilden die Kernaussage des Berichts. Im Glossar werden die verwendeten Hauptbegriffe erklärt und mit Beispielen erläutert.

[9] www.infraprotection.ch

3 Umfeldanalyse

Internationale Standards bilden die Grundlage für dieses Papier. Die International Standard Organisation (ISO) befasst sich in der 270xy-Serie mit Information- und IKT-Sicherheit[10]. Die North American Electric Reliability Corporation (NERC) behandelt im Critical Infrastructure Protection Standard (CIP) den Umgang mit Informationssicherheit[11]. Während die Standards der ISO 270xy-Serie eher generell die Informationssicherheit branchenübergreifend thematisieren, ist der Einsatz des Standards NERC CIP auf die Energiebranche und ICS fokussiert. Der Industrial Network and System Security Standard ISA / IEC 62443 regelt die ICS-Sicherheit umfassend auf allen Ebenen (Generelle Themen, Policys & Prozesse, Systeme und Komponenten).

Internationale Publikationen, wie etwa die Special Publication 800-82 «Guide to Industrial Control Systems (ICS) Security»[12] des National Institute of Standards and Technology und die Dokumentation «Analysis of ICS-SCADA IKT-Security Maturity Levels in Critical Sectors»[13] der European Union Agency for Network and Information Security (ENISA), zeigen internationale Bemühungen und Empfehlungen, um ICS auf ein höheres Schutzniveau anzuheben. Diese Publikationen richten sich an Fachkräfte und sind wenig geeignet, die Unterstützung des Top-Managements, der Verwaltungsräte und der Politik zu erreichen.

Nationale Publikationen werden von der Melde- und Analysestelle Informationssicherung MELANI[14] für den Bereich ICS sowie vom Bundesamt für Bevölkerungsschutz BABS[15] zum Schutz kritischer Infrastrukturen und den Auswirkungen auf die Gesellschaft und Wirtschaft zur Verfügung gestellt. Im Bundesamt für wirtschaftliche Landesversorgung BWL werden zudem aktuell Minimalstandards für die Stärkung der IKT-Resilienz der kritischen Versorgungsprozesse erarbeitet, welche auf dem obengenannten NIST-Framework aufbauen. Der vorliegende Bericht verstärkt die bisherigen Bemühungen von MELANI, BABS und BWL, um die Thematik einer breiteren Öffentlichkeit und den Vordenkern aus Wirtschaft, Behörden und Politik näher zu bringen.

[10] http://www.27000.org
[11] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[12] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf
[13] https://www.enisa.europa.eu/publications/maturity-levels
[14] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html
[15] www.infraprotection.ch

4 Empfehlungen

Untenstehend werden sieben Empfehlungen zur Sicherung der ICS vorgestellt. Nach Titel und Merksatz folgen Beschreibung, Ziel und Vorgehensweise. Die Zielgruppe für jede Empfehlung ist angegeben. Dabei ist wichtig, dass jede erwähnte Gruppe typischerweise eine spezifische Rolle hat: Die Politik muss Rahmenbedingungen setzen und fördern, Betreiber der Infrastrukturen müssen diese implementieren, Regulatoren müssen ihre Instrumentarien anwenden, Behörden müssen unterstützend oder führend sein, um eine Empfehlung umzusetzen.

4.1 Konsequente Analyse der Gesamtsysteme und bestehender Abhängigkeiten

Die konsequente Analyse des Gesamtsystems bestehender Abhängigkeiten und innewohnender Risiken ist eine zwingende Voraussetzung zum Identifizieren von kritischen ICS-Objekten.

Beschreibung: Einzelne kritische Infrastrukturen der Schweiz und damit ihre ICS sind hoch integriert; ICS-Komponenten werden immer häufiger und rascher verwendet und in übergeordnete Systeme integriert. Die Betreiber kritischer Infrastrukturen verfügen zwar meist über etablierte Instrumente, wie Risiko-, Kontinuitäts- oder Sicherheitsmanagementsysteme. Dass die Kontrollsysteme kritischer Infrastrukturen in bestehende, übergeordnete IT-Infrastruktursysteme mittels Netzwerken eingebettet sind und sich dadurch weitere Risiken ergeben, wird heute oft zu wenig beachtet. Aus ökonomischen Gründen steht die Betrachtung von betrieblichen (unternehmerischen) Risiken im Vordergrund, während die gesellschaftlichen Risiken oftmals vernachlässigt werden. Den Betreibern muss bewusst sein, dass ihr System Teil eines Ganzen ist und dass sich durch die Abhängigkeiten der Teile und Systeme untereinander Risiken ergeben, die im heute bestehenden betrieblichen Risikomanagement oft nicht adressiert werden (Common-Cause-Ausfälle und Kaskaden-Effekte, siehe Glossar). Als Beispiel dient das Schweizer Stromübertragungssystem als Teil des europäischen Verbunds. So können sich Ausfälle einzelner Systeme in der Schweiz nicht nur kaskadenartig im nationalen, sondern auch im europäischen Gesamtnetz ausbreiten. Umgekehrt kann sich ein Vorfall im europäischen Ausland auf die Schweiz auswirken. Die ENISA hat ebenfalls Anstrengungen für mehr ICS-Security[16] unternommen und empfiehlt den Mitgliedstaaten die Umsetzung. Wie dieses Beispiel zeigt, ist die ICS-Thematik national und international anzugehen, da es viele grenzüberschreitende Aufgaben gibt.

Ziel: Betreiber kritischer Infrastrukturen betrachten ihre Risikosituation und die Auswirkungen auf die Gesellschaft und Wirtschaft gesamtheitlich und gemeinsam mit den Behörden. Sie kennen bestehende ICS-Abhängigkeiten zwischen übergeordneten kritischen Infrastruktursystemen und den eigenen Systemen. Betreiber kritischer Infrastrukturen haben mögliche Auswirkungen auf ihr eigenes System geprüft und können im Bedarfsfall Massnahmen zur Begrenzung der Auswirkungen einleiten.

Vorgehensweise: Der «Leitfaden Schutz kritischer Infrastrukturen» des BABS[17] unterstützt Unternehmen und Behörden[18] in der Anwendung und Umsetzung einer gesamtheitlichen Risiko-Betrachtungsweise. Das BABS kann diese Arbeiten begleiten und stellt Kontakte zu den Fachstellen her, sodass die Risikosituation gemeinsam untersucht und die Verantwortung gegenüber der Gesellschaft abgestimmt wahrgenommen werden kann. Zur aktiven Stärkung der IKT-Resilienz erarbeitet das Bundesamt für wirtschaftliche Landesversorgung BWL zusammen mit Verbänden und weiteren Vertretern aus kritischen Versorgungsprozessen sowie Fachleuten aus dem Bereich der IKT-Security aktuell IKT-Minimalstandards, welche Unternehmen als handlungsleitende Empfehlung für den Betrieb ihrer kritischen IKT-Ressourcen dienen und ihnen über ein Benchmarking eine bessere Einschätzung ihrer ganzheitlichen Risikoexposition ermöglichen.
Für diese Empfehlung siehe auch ICS-Leitfaden MELANI[19]: Massnahme 10 «Security Incident Management Prozess» und Massnahme 11 «Sicherheitskultur etablieren»

Zielgruppe: Betreiber kritischer Infrastrukturen, Behörden

[16] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
[17] www.infraprotection.ch
[18] Voraussetzung für diese Unterstützung ist die Einschätzung als national kritische Infrastruktur, die den entsprechenden Unternehmen bekannt ist.
[19] https://www.melani.admin.ch/dam/melani/de/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf

4.2 Bewusster Umgang mit neuen risikoreichen Funktionalitäten

Potenzielle Vorfälle aufgrund neuer Funktionalitäten, z.B. Internet der Dinge, aufdecken, verhindern und deren Auswirkungen vermindern.

Beschreibung: Die Systemlandschaft ist massiven strukturellen, operationellen und technologischen Änderungen unterworfen: Zuvor getrennte Systeme wachsen zu einem «System of Systems» zusammen. Zudem ist ein Trend zur Dezentralisierung und «Smartness» zu beobachten. Beispiele dafür sind Privathaushalte als Stromerzeuger und -verbraucher und Teilnetzkontrolleur oder die private Gebäudeautomation. Aufkommende Technologien, zu denen auch das autonome Fahren gehört, erzeugen des Weiteren neue Akteure und Geschäftsmodelle, die in die Risikobetrachtung zu integrieren sind. Bei den hoch dynamischen Veränderungen spielen ICS eine entscheidende Rolle und führen – neben unbestreitbaren Vorteilen hinsichtlich verbesserter Kommunikation und Systemführung – zu neuen Gefahren und Risiken. Weitreichende Fragen bezüglich ausreichender Zuverlässigkeit der ICS und deren Validierung sind heute noch nicht zufriedenstellend beantwortet.

Ziel: Potenzielle Vorfälle, die durch risikoreiche neuartige Funktionalitäten in Geräten und Systemen auftreten, dank kontinuierlichem Risikomanagement aufdecken und mit geeigneten Gegenmassnahmen verhindern oder die Auswirkungen vermindern.

Vorgehensweise: WLAN und nicht validierte Sicherheitsfunktionen wie Firewalls sollen bei Inbetriebnahme neuer Systemkomponenten abgeschaltet werden. Dadurch kann verhindert werden, dass neue Komponenten als Eintrittstor für unerwünschte Vektoren dienen. Autonom operierende Algorithmen in Systemen müssen vor der Markteinführung ausreichend validiert und systemübergreifend getestet sein. Die Risikobetrachtung soll als kontinuierlicher Prozess gelebt werden: Bekannte Risiken sollen periodisch neu eingeschätzt und aufkeimende Risiken so früh als möglich erfasst werden. Ein lagegerechtes Risikobewusstsein soll geschaffen und Sicherheitsmassnahmen sollen gemäss der Risikolage vorgesehen werden. Entsprechende Zertifizierungen von Komponenten sind in der ENISA in Vorbereitung[20].
Für diese Empfehlung siehe auch ICS-Leitfaden MELANI: Massnahme 10 «Security Incident Management Prozesse»[21]

Zielgruppe: Betreiber kritischer Infrastrukturen, Behörden, Regulatoren

4.3 Robustheit und Resilienz stärken

Die Stärkung von Robustheit und Resilienz ist der Ausgangspunkt, um Systeme sicher und im Ereignisfall mit minimalen Unterbrüchen zu betreiben.

Beschreibung: Eine hohe Verfügbarkeit und Robustheit von Daten, Prozessen und Systemen der Informations- und Kommunikationstechnologie (IKT) gegen einen potenziellen Ereignisfall ist für das Funktionieren der Steuerung kritischer Systeme von höchster Bedeutung. Schon bei einer nur temporär eingeschränkten Verfügbarkeit drohen Folgeschäden für unsere Gesellschaft und/oder Wirtschaft, z.B. nicht realisierte Geschäfte, Verzögerungen und Verluste wegen Produktionsunterbruch. Dabei stehen zwei Punkte im Vordergrund: die Robustheit gegen Angriffe und Bedrohungen, sodass diese möglichst keine oder wenig Wirkung zeigen und die Resilienz, die zusätzlich zum Schutz auch eine stringente Überwachung des korrekten Funktionierens und Massnahmenpläne für Fehlerfälle beinhaltet, die dann die Auswirkungen auf das Geschäft minimieren sollen.
Die Prozessketten werden zunehmend länger und auch breit verstreut: Sie umfassen Produzenten, Lieferanten, Logistiker und auch den effektiven Verkauf. Beim Verkauf werden Daten erhoben, die Nachbestellungen beim Lebensmittelproduzenten bzw. -lieferanten auslösen und auch zu Statistik und Prognosezwecken (Cumulus, Supercard) verwendet werden. Diese Prozessketten hängen von Infrastrukturen wie Logistikknotenpunkten, Telekomdienstleistern und Verteilzentren ab. Fallen diese Infra-

[20] E.g.: https://www.enisa.europa.eu/publications/good-practices-for-an-eu-ics-testing-coordination-capability

[21] https://www.melani.admin.ch/dam/melani/de/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf

strukturen aus, steht die ganze Prozesskette still beziehungsweise muss auf andere, weniger effiziente Betriebsmodi umgestellt werden. Dabei entstehen oft grössere Schäden, Mehrkosten und Verzögerungen.
Ein Beispiel ist der Lebensmittelsektor. Dieser weist eine hohe Vernetzung sowohl innerhalb der Branche (Produktion, Lager, Filialstandorte, Logistik, Detailhandel) als auch zu anderen Sektoren (Energie, Kommunikation, Industrie) auf. Der Lebensmittelsektor ist heute stark von ICS abhängig. Versorgungsrelevante Akteure der Branche sind oftmals gar nicht in der Lage, selbst umfassende Risikoanalysen – unter Berücksichtigung der gesellschaftlichen Folgen – vorzunehmen und eigenständig Sicherheitsmassnahmen umzusetzen. Oft befinden sich essenzielle Systeme für die Lebensmittelversorgung ausserhalb der Branchenkontrolle, z.B. bei Lieferanten und Logistikern. Für die systemweite Risikoanalyse über Prozessketten, die viele unterschiedliche Partner und Betriebe umfassen, ist es deshalb empfehlenswert, externe professionelle Hilfe beizuziehen.
Neben der Verfügbarkeit ist die Integrität der Daten ein mindestens ebenso wichtiger Aspekt für die Sicherstellung der Funktionsweise von ICS. Datenveränderungen müssen technisch erkannt werden, um eine Manipulation von Parametern in ICS frühzeitig aufdecken zu können. Eine Datenmanipulation kann weitreichende Konsequenzen haben, wie etwa den Ausfall von Systemen. Als klassisches Beispiel dafür ist das Schadprogramm Stuxnet zu nennen, das u.a. die Zerstörung der Zentrifugen der iranischen Urananreicherung zur Folge hatte. Etwas simplifiziert können auch praktische Auswirkungen genannt werden, z.B. der Ausfall des automatischen Melkens der Kühe und fehlendes Personal, um die Kühe von Hand zu melken, sowie die Kühl- und Gefrierhäuser, die nicht mehr kühlen, wodurch grosse Mengen Lebensmittel verderben und entsorgt werden müssen.

Ziel: Verfügbarkeit von IKT-Daten, -Prozessen und -Systemen so gut wie möglich sicherstellen. Integrität der Daten gewährleisten.

Vorgehensweise: Betreiber von kritischen Systemen sollen ihre IKT, also Hardware, Software, Prozesse, Dienste und Daten, in mindestens zwei geo-redundanten Rechenzentren in der Schweiz betreiben, die beide jeweils mindestens die Anforderungen des Tier III Standards (siehe Glossar) erfüllen. Zur Sicherstellung der Integrität der Daten sollen geeignete technische Massnahmen ergriffen werden, z.B. die Bildung eines Integritätscodes (hash value), der die Originaltreue der Daten feststellt.
Für diese Empfehlung siehe auch ICS-Leitfaden MELANI: Massnahme 4 «Robuste Netzwerkarchitektur» und Massnahme 11 «Sicherheitskultur etablieren»[22]

Zielgruppe: Behörden

4.4 Security by Design

Security by Design soll für alle neuen ICS direkt angewendet werden, um Unsicherheit und teures Aufrüsten von Sicherheit zu vermeiden[23].

Entsprechend der Natur von IKT-Architekturen braucht es sehr viele Sicherheitsregeln. Deshalb ist diese Empfehlung so umfangreich und von der Struktur her anders als die anderen. Untenstehend werden jedoch nur die elementarsten und wichtigsten Regeln der «Security by Design» wiedergegeben.

Beschreibung: Viele kritische Systeme sind untereinander vernetzt und miteinander verknüpft, wobei ein ganz wesentlicher Teil der Verknüpfung über ICS erfolgt. Beispiele für solche Verknüpfungen in verschiedenen Sektoren sind:
- Verknüpfung von Strom-Handelssystemen mit den ICS für Netzsteuerung (Energiesektor).
- Direkte Übertragung von Produktionsdaten in SAP-Systeme für Auswertungen und Produktionssteuerung (Industriesektor).
- Verknüpfung von Diagnosegeräten und lebenserhaltenden Systemen (Medizinal-Technologie) mit der Patien-

[22] https://www.melani.admin.ch/dam/melani/de/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf

[23] Security by Design bezieht sich auf Sicherheitsregeln der Architektur von Komponenten und Systemen.

tenadministration im Spital («Geschäfts-IT») und in Zukunft auch mit der schweizweit verfügbaren elektronischen Patientenakte «e-Health» (Gesundheitswesen).
- Vernetzung der Verkehrsleitsysteme durch den zentralen Betrieb des schweizerischen Nationalstrassennetzes (Strassenverkehr).

Neuere Kontrollsysteme basieren auf kommerzieller Hard- und Software. Falls diese in kritischen Infrastrukturen eingesetzt werden und in einem dieser Systeme ein Fehler auftritt, kann dies ein multiples (dezentrales) Systemversagen mit gravierenden nationalen Auswirkungen nach sich ziehen.

Bei bestehenden ICS ist die Langlebigkeit eine Schwierigkeit. Man rechnet mit einem Lebenszyklus von 25 bis 40 Jahren, sodass ein Nebeneinander von «alter» und «neuer» Technologie entsteht. Ältere Systeme waren ursprünglich ohne Internetanschluss gebaut. Nachträgliche Anbindungen ans Internet haben oft keine oder nur ungenügende IKT-Security-Funktionen. Es ist daher essenziell, eine resiliente Sicherheitsarchitektur anzuwenden und mit sicherer Hard- und Software zu arbeiten[24]. Wo kommerzielle Software eingesetzt wird, ist der vom Hersteller vorgegebene Lebenszyklus zu berücksichtigen. Somit sind auch Mittel zu budgetieren, um die ICS jeweils auf den Stand der Technik (Sicherheitssupport) nachzuführen.

Ziel: Multiples (dezentrales) Systemversagen aufgrund von Architekturmängeln und Fehlern in Hard- und Softwareentwicklung verhindern.

Vorgehensweise: Den Grundsatz Security by Design anwenden. Dies beinhaltet, soweit möglich, die Anwendung folgender Prinzipien bei der Entwicklung von Hard- und Software für ICS:

- **Fehlertoleranz:** Ein einzelner Fehler darf nicht zum Verlust der Verfügbarkeit des Systems führen.
- **Ausfallsicherheit** ist ein Konzept der Verfügbarkeit und minimiert die Unterbrüche eines Service.
- **Ausfallrisikominimierung** (fail safe) behält das System auch bei Ausfällen in sicherem Zustand. Beispiel dafür sind die Züge der SBB, die bei einem Vorfall stoppen und so in einen sicheren Zustand übergeführt werden.
- **Redundanter Systemaufbau** mit **verschiedenartigen Systemkomponenten** (Komponenten von verschiedenen Herstellern mit unterschiedlicher Architektur): Auf diese Weise werden die Auswirkungen eines systematischen Ausfalls eines Typs von Systemkomponenten begrenzt und der «Common-Cause-Effekt» reduziert.
- **Hoher Automatisierungsgrad:** Dieser reduziert den Einfluss menschlicher Fehlhandlungen. Dennoch sollte der Mensch in unvorhergesehenen Vorfällen eingreifen können.
- **Verzicht auf die Nutzung des öffentlichen Internets** und von Verbindungen zum öffentlichen Internet, sofern diese nicht ausreichend gesichert worden sind. Ein «Inselbetrieb» kann das Risiko von IKT-Angriffen reduzieren, so er konsequent durchgeführt wird – d.h. kein Anschluss von Hardware (z.B. USB-Sticks oder andere mitgebrachte Hardware), die nicht Teil der ursprünglichen Lösung ist.
- **Anwenden von sicheren Systemarchitekturen**, die für jede Risikostufung geeignete Sicherheitszonen[25] vorsehen, mit dem Ziel, gegenseitige Beeinflussungen der Zonen zu eliminieren und dadurch eine höhere Sicherheit zu generieren. Die Sicherheitszonen werden in Kraftwerken üblicherweise wie folgt gewählt:
  - Separate Zone für Leittechnik (SCADA)
  - Separate Zone für Markt-Daten
  - Separate Kontroll-Zone für Unterwerke
  - Separate Kraftwerk-Kontroll-Zone
  - Separate Zone für die Planung
  - Separate Zone für Internet der Dinge
- **Strategien und Konzepte** für die Sicherstellung der «Post-Market»-Sicherheit von ICS. Neben automatisiertem Patch- und Change-Management gehören dazu aufgrund der langen Betriebsdauern auch Konzepte für Aktualisierung und Auswechslung der Hardware.
- **Security by Design und sicheres Programmieren** in allen relevanten Aus- und Weiterbildungsangeboten aller Ausbildungsstufen als festen Bestandteil integrieren. Gleichzeitig die Inhalte als berufliche Weiterbildung anbieten[26,27]

24 https://library.e.abb.com/public/286f6a0d155f468e85060039b697d1a9/Bridging%20IT%20and%20OT_survey%20report_Apr16.pdf

25 Eine Unternehmung wird aufgrund unterschiedlicher Risiken in Zonen aufgeteilt, z.B. Besucherzone, Mitarbeiterzone, Serverzone, Tresorzone. Diese Zonen nennt man Sicherheitszonen.

26 https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

27 https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#43b62ee85163

Für diese Empfehlung siehe auch ICS-Leitfaden MELANI: Massnahme 2 «Umgang mit Software», Massnahme 4 «Robuste Netzwerkarchitektur» und Massnahme 5 «Mehrstufiger Malware-Schutz»[28]

Zielgruppe: Behörden und Fachvereinigungen (Fördern der Akzeptanz der «Security by Design»); Ausbildungsverantwortliche, Ausbildungsprogrammverantwortliche an Hochschulen (Wissen zu «Security by Design» weitergeben); Betreiber kritischer Infrastrukturen, Entwickler, Projektleiter mit Evaluationsverantwortung («Security by Design» implementieren)

4.5 Schulung der Mitarbeitenden

Schulung vermeidet Fehler und ist eine effiziente und kostengünstige Massnahme.

Beschreibung: Zum heutigen Zeitpunkt ist es schwierig, Mitarbeitende zu finden, die sich der Problematik bewusst sind, die mit ICS in kritischen Systemen einhergehen. Dies lässt sich anhand von Expertenmeinungen und Publikationen über den Fachkräftemangel feststellen. Da kritische Systeme zunehmend IT und ICS anwenden und in der IT grundsätzlich eine hohe Personalfluktuation besteht, entstehen zusätzliche Sicherheitslücken: Passwortwechsel, Vertraulichkeit von Sicherheitsmassnahmen, Prozesskenntnisse und Schwachstellen, die nicht nur missbräuchlich, sondern auch durch Personalumwälzung nach aussen gelangen. Zudem sinkt vielerorts die Identifikation der Mitarbeitenden mit ihrem Arbeitgeber, insbesondere im Dienstleistungssektor. Durch mehrfach verschachteltes Outsourcing der Dienstleistungen nimmt auch das Risiko von Insider-Taten laufend zu.

Ziel: Klar ist, dass die Vorgesetzten diesbezüglich eine Vorbildfunktion wahrnehmen müssen. Ausserdem sind gut ausgebildete und motivierte Mitarbeitende sehr wichtig, die sich den Herausforderungen bewusst sind, welche ICS in kritischen Systeme mit sich bringen. Mitarbeitende, die direkt mit ICS arbeiten, müssen deren Security sowie deren IKT-Security beherrschen. ICS-Security- Zertifizierungen[29,30] für Experten könnten eine gewisse Kompetenz-Transparenz für Unternehmensverantwortliche schaffen.

Vorgehensweise: Die Verantwortung für die Sicherheit der ICS muss innerhalb der Unternehmen einen hohen Stellenwert haben und in der Firmenhierarchie entsprechend hoch angesiedelt sein. Dabei müssen für Sicherheitsmassnahmen adäquate Mittel und Möglichkeiten zur Verfügung stehen. Ein besonderes Augenmerk gilt den Mitarbeitenden. Diese müssen geschult werden, sodass alle bewusst und motiviert einen Beitrag zur Sicherheit leisten können. Für diese Empfehlung siehe auch ICS-Leitfaden MELANI: Massnahme 6 «Authentisierung und Autorisierung»[31]

Zielgruppe: Betreiber kritischer Infrastrukturen, Aus- und Weiterbildungsinstitutionen

4.6 Aufbau eines Schweizer ICS Computer Emergency Response Team (CERT)

Der Aufbau eines ICS CERT ist für eine hohe ICS-Sicherheit eine zentrale Voraussetzung. Ein Schweizer ICS CERT ist eine Möglichkeit, diesen Prozess optimal zu begleiten.

Beschreibung: Die kontinuierliche Professionalisierung der organisierten Cyber-Kriminalität und die Digitalisierung von Gesellschaft und Wirtschaft führen zur Auflösung von Sicherheitsperimetern. Eine rein präventive Sicherheitsarchitektur reicht für einen adäquaten Schutz kritischer Systeme nicht mehr aus. Darum werden folgende Punkte immer wichtiger: Erkennen von Eindringlingen, Reaktionsfähigkeit bei Vorfällen, Kenntnis über relevante Angreifer und Angriffe und zugehörige, spezifische sowie einzigartige Indikatoren. Diese Punkte gehören zu den Kernkompetenzen eines CERT.

[28] https://www.melani.admin.ch/dam/melani/de/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf

[29] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

[30] https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

[31] https://www.melani.admin.ch/dam/melani/de/dokumente/2013/10/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf.download.pdf/massnahmen_zum_schutzvonindustriellenkontrollsystemenics.pdf

Ziel: Aufbau und Betrieb eines ICS CERT in der Schweiz, um der Bedrohungsentwicklung mit Eigenverantwortung entgegenzutreten und das notwendige Schutzniveau sowie die Reaktionsfähigkeit zu erreichen.

Vorgehensweise: Der Aufbau und Betrieb eines CERT ist zeitintensiv und erfordert hochspezifisches Wissen, das nur von entsprechenden Spezialisten geliefert werden kann. Ein CERT setzt das Vertrauen der Akteure sowie nationale und internationale Vernetzung voraus. Daher sollen für den Aufbau etablierte, vertrauenswürdige Organisationen – also bestehende Kompetenzzentren – genutzt werden, um Synergieeffekte zu verstärken und Kosten tief zu halten. Der initiale Aufbau muss mit klarem Fokus und klaren Spielregeln in enger Zusammenarbeit mit wenigen Schlüsselunternehmen erfolgen und später in einem geeigneten Setup auf weitere Unternehmen ausgeweitet werden. Möglich sind verschiedene Modelle: So können etwa nur Vertreter eines Sektors, Vertreter eines Sektors und Behörden oder aber Vertreter aus verschiedenen Sektoren und Behörden am initialen Aufbau beteiligt sein. Innerhalb des Energiesektors wäre der Aufbau eines ICS CERT wohl am raschesten akzeptiert und möglich, weil der potenzielle Nutzen von den Experten als gross eingeschätzt wird.
Bezüglich eines ICS Energie CERT wurde auch die Arbeitsgruppe ICS Security des Verbands Schweizerischer Elektrizitätsunternehmen (AG ICS VSE) kontaktiert, die zurzeit Standards für die Elektrizitätsbranche erarbeitet. Die Anliegen der AG ICS VSE auf Stufe Konzeption und Umsetzung eines ICS Energie CERT werden die vorliegenden Empfehlungen gut ergänzen und positionieren.

Zielgruppe: Betreiber kritischer Infrastrukturen, Behörden, Politik

4.7 Internationale Vernetzung und Informationsaustausch

Internationale Vernetzung und Informationsaustausch in Vertrauensgemeinschaften gelten als bevorzugte Methoden, um hohe Sicherheit zu erzeugen.

Beschreibung: Ein Alleingang bezüglich Sicherheit industrieller Kontrollsysteme ist nicht zielführend, da die Schweiz in einen Gesamtkontext eingebunden ist. Unter Experten ist allgemein anerkannt, dass der vertrauensvolle Austausch von sicherheitsrelevanten Informationen einen grossen Beitrag zur Stärkung der Sicherheit leistet.

Ziel: Die Sicherheit ist durch internationale Zusammenarbeit und Informationsaustausch gestärkt.

Vorgehensweise: Die Schweiz soll aktiv an internationalen Aktivitäten wie NATO-Cyber-Security-Übungen teilnehmen sowie sich an Kompetenzzentren und am gegenseitigen Austausch von sicherheitsrelevanter Information beteiligen. Die Teilnahme in internationalen Gremien ermöglicht eine Standortbestimmung und Anschluss an den Informationsaustausch, sodass neue Entwicklungen und Trends frühzeitig erfasst werden können. Eine mögliche Basis dafür sind die Umsetzungsarbeiten im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS, M11)[32], geführt durch das Bundesamt für Kommunikation BAKOM.

Zielgruppe: Betreiber kritischer Infrastrukturen, Behörden, Regulatoren

[32] http://www.news.admin.ch/NSBSubscriber/message/attachments/39698.pdf Seite 15

5 Glossar

Kritische Infrastrukturen

Hier wird die Definition der Schweiz wiedergegeben: Ausfall, Störung oder Zerstörung kritischer Infrastrukturen haben gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat. Diese Definition für kritische Infrastrukturen hat der Bundesrat 2012 im Rahmen der Nationalen Strategie zum Schutz kritischer Infrastrukturen SKI (SKI-Strategie) verabschiedet[33].

Auf www.Infraprotect.ch werden folgende charakteristische Merkmale für Objekte mit grosser Kritikalität definiert:

- Keine oder nur begrenzte Möglichkeit einer Substitution im Ereignisfall;
- Hoher Vernetzungsgrad mit Abhängigkeiten zu Infrastrukturen in anderen (Teil-)Sektoren;
- Direkte und indirekte volkswirtschaftliche Risiken mit grosser Bedeutung für die Schweiz;
- Aus nationaler Sicht systemrelevant und essenziell für unsere Gesellschaft.

Robustheit und Resilienz [34]

Ein robustes System besitzt die Fähigkeit, Veränderungen standzuhalten, ohne dass dabei seine anfänglich stabile Struktur verändert wird. Das System vermag somit auch unter ungünstigen Bedingungen (z.B. Fehlbedienung) noch zuverlässig zu funktionieren.

Die Resilienz bezieht sich gemäss SKI-Strategie auf die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen (Widerstandsfähigkeit) und die Funktionsfähigkeit möglichst zu erhalten (Anpassungsfähigkeit) respektive möglichst schnell und vollständig wiederzuerlangen (Regenerationsfähigkeit).

Die Fähigkeit von kritischen Infrastrukturen, nach einer Störung wieder in die normale Funktion zurückzukehren, setzt sich gemäss nationaler Strategie zum Schutz von kritischen Infrastrukturen aus vier Bestandteilen zusammen:

1. Die Robustheit der Systeme (z. B. kritische Infrastrukturen, Staat, Wirtschaft und Gesellschaft) an sich
2. Die Verfügbarkeit von Redundanzen
3. Die Fähigkeit, wirksame Hilfsmassnahmen zu mobilisieren
4. Die Schnelligkeit und Effizienz der Hilfsmassnahmen

Industrielle Kontrollsysteme ICS

Unter Industriellen Kontrollsystemen (Industrial Control Systems, ICS) werden unterschiedliche Typen von Kontrollsystemen verstanden, wie Leitsysteme (Supervisory Control and Data Acquisition Systems, SCADA-Systeme) und verteilte Kontrollsysteme (Distributed Control Systems, DCS). Sie dienen beispielsweise der Überwachung oder der Steuerung von Produktionsanlagen oder ganzer Netzwerke wie dem Stromübertragungssystem.

Common-Cause-Ausfälle

Mit dem Common-Cause-Effekt wird das Phänomen beschrieben, dass es aufgrund gemeinsamer Ursachen zu einem multiplen Komponenten- oder Systemversagen kommt, mit gravierenden Auswirkungen kommt. Ein Beispiel für den Effekt ist ein gezielte IKT-Angriff auf industrielle Kontrollsysteme gleicher Bauart gleichzeitig auf mehrere Stromlieferanten. Als Folge dessen kann die Stromversorgung in mehreren geografischen Bereichen gleichzeitig ausfallen.

Kaskadeneffekt

Allgemein ist ein Kaskadeneffekt eine Abfolge von Ereignissen, von denen jedes einzelne zugleich Ursache des folgenden ist und alle auf ein einzelnes Anfangsereignis zurückgehen. Im einfachsten Fall besteht die Kaskade nur aus zwei Elementen, was als Abhängigkeit bezeichnet wird. Beziehen wir uns auf den unter Common-Cause-Effekt beschriebenen Stromausfall in mehreren geografischen Bereichen. Die Folge ist, dass die Kommunikation in den betroffenen Gebieten weitestgehend ausfällt. Der Ausfall der Kommunikation bewirkt, dass die Verkehrssteuerung nicht funktioniert und auch die Logistik ausfällt (z.B. alle Prozessketten der Lebensmittelversorgung).

[33] www.infraprotection.ch

[34] Hier ist die Schweizer Definition wiedergegeben. Internationale Definitionen weichen davon ab. Siehe z.B. Eur | Secur Res (2017), Wolfgang Kröger

Tier Standard

Zur Bewertung des Sicherheitsniveaus von Rechenzentren hat sich weltweit der so genannte «Tier Standard» des US-amerikanischen Uptime Institute durchgesetzt, der die Sicherheit von Rechenzentren anhand einer vierstufigen Skala von «Tier I» bis «Tier IV» bewertet. «Sicherheit» wird dabei umfassend verstanden. Die untersuchten und bewerteten Faktoren sind vielfältig und enthalten physischen Zugriffsschutz (Perimeterschutz, Biometrische Zugangskontrollen, etc.), die Art der Stromversorgung (mehrfach redundante Stromversorgung, Notstromaggregate vorhanden, etc.), Typ der verbauten Brandschutzanlagen und viele weitere Faktoren.

Security by Design

Security by Design bedeutet, dass Sicherheitsgrundsätze in der Software- und Hardware-Entwicklung vom ersten Schritt der Planung an angewendet werden. Der Sicherheitsaspekt wird dadurch zu einem fundamentalen Kriterium bei der Auswahl der Entwicklungswerkzeuge bis zur endgültigen Produkteinführung. Nur so können Sicherheitslücken vermieden und die Risiken für die Anwender, beziehungsweise die Gesellschaft, reduziert werden.

satw it's all about technology

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Projektleiter
Bernhard Hämmerli
Autoren
Stefan Brem, Daniel Caduff, Monica Duca Widmer, Martin Leuthold, Esther Koller-Meier, Wolfgang Kröger, Rita Hofmann, Matthias Kaiserswerth, Pascal Lamia, Rajesh Nair, Daniel Rudin, Ruedi Rytz, Stephanie Teufel, Gérald Vernez, Nicole Wettstein

www.satw.ch
November 2017