pexels-manuel-geissinger-325229

Räumliche Trennung bei der Digitalisierung von Kritischen Infrastrukturen?

https://ag.kritis.info/2020/10/15/
raeumliche-trennung-bei-der-digitalisierung-von-kritischen-infrastrukturen/

AG KRITIS

15. Oktober 2020

Es ist nicht klug, so das Sprichwort, alle Eier in einem Korb zu lagern. Eine grundlegende Vorsichtsmaßnahme gegen Unfälle und Missgeschicke, aber auch gegen Angriffe, ist die räumliche Trennung von Werten. Insbesondere werden kritische Komponenten grundsätzlich redundant ausgelegt und diese redundanten Systeme räumlich voneinander getrennt betrieben, um zu vermeiden dass ein einzelnes Ereignis einen Schaden anrichten kann.

Es wird niemanden überraschen, dass die fortschreitende Digitalisierung und Vernetzung von Systemen der Kritischen Infrastruktur die Schutzwirkung von Redundanz und räumlicher Trennung deutlich schwächt. Für digitale Angreifer stellt Redundanz alleine kein Hindernis dar, wenn die redundanten Systeme dieselben Schwachstellen aufweisen. Und die Kommunikation in der digital vernetzten Welt koppelt räumlich getrennte Systeme wieder so dicht zusammen, wie schnell Daten durch das Kommunikationsnetz gesendet werden können. Eine unabsichtliche Fehl-Fernbedienung oder ein absichtlicher Angriff können digitalisierte, redundante Komponenten gleichermaßen betreffen.

In diesem Artikel diskutieren wir die Schwächung physischer Barrieren durch Digitalisierung und mögliche Maßnahmen zur Sicherstellung eines grundlegenden Schutzniveaus einer digitalisierten Kritischen Infrastruktur.

Physische Trennung als traditionelle Schutzmaßnahme

Physische Trennung in den verschiedensten Ausprägungen ist eines der am weitesten verbreiteten Schutzkonzepte, um Schaden zu vermeiden oder zumindest das Schadensausmaß zu reduzieren. Die Techniken sind dabei so vielfältig wie für uns alltäglich und intuitiv, dass wir sie vielleicht nicht einmal wirklich als solche erkennen. Ein Beispiel für so eine intuitive räumliche Trennung sind Bürgersteige und Fahrspuren, während Ampeln eine ebenso intuitive zeitliche Trennung darstellen.

Auch Kritische Infrastruktur wird in wesentlichen Teilen durch physische Trennung geschützt, sei dies die räumliche Barriere um ein Kraftwerk oder die räumlich getrennte redundante Stromversorgung eines Krankenhauses. Auch die durch Ressourcen-Lagerung erreichte zeitliche Trennung der Verbraucher von den Versorgungsquellen ist ein wesentlicher Baustein traditioneller Schutzkonzepte.

Schaden mit nahezu Lichtgeschwindigkeit

Digitalisierung von Kritischer Infrastruktur bedeutet vor allem einen automatisdocumentierten Austausch, sowie die Erzeugung und Verarbeitung von Sensor- und Steuerdaten. Insbesondere die hohe Geschwindigkeit der Kommunikation, zwischen 50 und 90

Allein in diesem Jahr finden sich etliche öffentliche Berichte von Firmen, Universitäten, Gerichten, kommunalen Systemen als auch Universitätskliniken und Krankenhäusern, die durch Ransomware innerhalb kürzester Zeit für Tage oder Wochen vollständig lahmgelegt wurden. Was selbst eine massive Sabotage an der Stromversorgung nicht erreichen könnte, bewirkt die Schadsoftware der organisierten Kriminalität in Minuten. Traditionelle Schutzkonzepte, die nur auf Redundanz und physischer Trennung beruhen, sind in einer digitalisierten Infrastruktur offensichtlich unzureichend.

Digitalisierte Schutzkonzepte

Die wesentliche Frage ist also, wie die physische Trennung ergänzt werden kann, um sowohl gegen Fehler als auch gegen Angriffe in einer digitalisierten Infrastruktur zu schützen? Sehr abstrakt betrachtet ist dies ein Kernthema der IT-Sicherheit, in deren Entwicklung eine Vielzahl von Schutzmechanismen erarbeitet wurden, mit denen physische Mechanismen ersetzt oder ergänzt werden. Die „Firewall“ hat es als dominantere Technologie sogar bis in den allgemeinen Sprachgebrauch geschafft. Im Folgenden werden einige Konzept vorgestellt, die in der IT-Sicherheit entwickelt wurden, um die Auswirkungen von Angriffen und Fehlern zu limitieren und zu verringern.

Isolation & Kapselung

Auch wenn es verlockend bzw. kostengünstiger erscheint, Systeme großflächig einheitlich zu digitalisieren, sollte nicht einfach „alles mit allem“ vernetzt werden. Der Grad der Vernetzung sollte sich an dem konkret vorgesehenen Kommunikationsbedarf orientieren. Systeme unterschiedlicher Kritikalität sollten auch im digitalen grundsätzlich voneinander getrennt bleiben. Kommunikation sollte nur in dem Maße ermöglicht werden, wie Bedarf und Nutzen nachgewiesen werden – sog. Business need to Know Designprinzip. Insbesondere sollen redundante Komponenten nicht über dieselben Kommunikationsnetze steuerbar bzw. erreichbar sein.

Eng verbunden mit dem Designprinzip der Isolation ist auch das „least privilege“ Designprinzip, das die Zugriffsmöglichkeiten und Rechte auf den einzelnen Systemen in ähnlicher Weise auf das Notwendige einschränkt.

Unabhängigkeit

Jede Abhängigkeit eines digitalen Systems bedeutet auch eine weitere potentielle Angriffsfläche. Auch die möglichen Fehlerquellen werden schnell unüberschaubar. Daher sollten Systeme in Kritischen Infrastrukturen möglichst unabhängig von anderen Systemen, Diensten und Funktionen betrieben werden. Ist eine Abhängigkeit notwendig, sollte diese als ebenso kritisch berücksichtigt werden. Benötigt ein System beispielsweise die exakte Uhrzeit, lässt sich eine Abhängigkeit zu einem Zeit-Server nicht vermeiden. Dieser Zeit-Server muss dann in das Schutzkonzept gegen Angriffe und Fehler mit einbezogen werden.

Heterogenität

Zuerst einmal sollte akzeptiert werden, dass Teile eines Systems ausfallen oder kompromittiert werden können. Insbesondere muss geplant werden, dass gleichartige Komponenten mit höherer Wahrscheinlichkeit gleichzeitig betroffen sind, weshalb Backup- und Wiederherstellung für den Ausfall ganzer Komponentengruppen geplant, umgesetzt und (auch die Wiederherstellung) getestet werden müssen.

Digitalisierte Systeme bestehen heutzutage jeweils aus einem komplexen Stapel von Software- und Hardware-Komponenten. Eine wesentlich Erkenntnis ist,

dass Schwachstellen einer Komponente dieses Stapels meist alle Systeme betreffen, in denen diese Komponente verwendet wird. Die weite Verbreitung einer Komponente, z. B. eines Betriebsystems oder einer beliebten Softwarebibliothek führt dazu, dass auch deren Schwachstellen weit verbreitet sind und die betroffene System dementsprechend angreifbar wären. Um die Auswirkungen einzelner Schwachstellen zu reduzieren ist es demzufolge wichtig, die Verbreitung gleichartiger Baureihen zu beschränken, kurz, die

Infrastruktur aus Systemen mit möglichst unterschiedlichen Software- und Hardware-Komponenten aufzubauen. Damit würde Heterogenität als eine digitale Schutztechnik die Redundanz bzw. räumliche Trennung ergänzen.

Praktisch bedeutet Heterogenität aber auch, dass der Aufwand in der Herstellung und subsubsectionim Betrieb der Infrastruktur steigt. Offensichtlich kann nicht jedes System vollständig anders als alle anderen aufgebaut werden. Deshalb ist es zuerst wichtig, eine Abwägung zu treffen und minimale Heterogenitätsanforderungen zu definieren. Dabei kann weiterhin der, oft durchaus räumlich beschränkte, Wirkbereich von Systemen berücksichtigt werden. Eine einfache Verteilung gleichartiger Komponenten auf unterschiedliche Systeme führt nämlich auch dazu, dass alle Systeme gleichzeitig angreifbar werden. Diese Abschätzung fehlt bisher in allen wesentlichen Standards und Richtlinien für den Schutz von Systemen.

Bei einigen Technologien ist Heterogenität nur in geringem Maß umsetzbar. In diesem Fall ist neben erhöhten Isolations- und Unabhängigkeitsanforderungen auch eine bessere Reaktivität notwendig.

Reaktivität

Im Vergleich zu nicht digitalisierter Kritischer Infrastruktur unterliegen Hardware und insbesondere Software heutzutage sehr kurzen Lebenszyklen. Wöchentliche Updates und monatliche „Patchdays“ sind eher die Regel als die Ausnahme. Gleichzeitig gilt das Betreiben möglichst aktueller Software und Hardware als beste Maßnahme gegen Angriffe. Dies ist schon in einem Büro-IT Umfeld schwierig. Digitale Kritische Infrastruktur schnell und häufig zu aktualisieren wird in den meisten Fällen ein enorme Herausforderung sein. Gleichzeitig stellt dies sogar ein wesentliches Risiko für die Verfügbarkeit der Versorgung dar. Trotzdem gehört die Reaktivität auf neue Schwachstellen als auch aktualisierte Software und Hardware in jedes Schutzkonzept. Möglichst frühzeitig sollte das eigene Reaktionsvermögen – unter anderem auf Schwachstellen und veraltete Komponenten – realistisch abgeschätzt werden. Dieses (vermutlich nicht allzu schnelle) Reaktionsvermögen sollte dann die Basis für die Planung von Betriebs- und Wartungszyklen sein. Ebenso sollte der Schutzbedarf gemäß den vorher vorgestellten Konzepten daran ausgerichtet werden, wie viele Schwachstellen innerhalb eines Betriebszyklus zu erwarten sind, ohne diese reaktiv beheben zu können.