CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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

WISSENS-UPDATE

Kritische Infrastrukturen: wunde Punkte in der Cyber Security

Ohne Kritische Infrastrukturen funktioniert nichts. Störungen in Spitälern, der Wasser- oder Energieversorgung können für Wirtschaft und Gesellschaft dramatische Folgen haben. Zudem lösen sie eine Kettenreaktion aus – auch ein kleinflächiger Stromausfall hat weitreichende Konsequenzen, wenn er Teile der Telekommunikation oder des Schienenverkehrs ausser Kraft setzt. Jüngere Ereignisse zeigen: Die Gefahr für solche Ausfälle steigt.

2017 befällt die Schadsoftware «WannaCry» weltweit Kritische Infrastrukturen. Im September 2020 kommt der Betrieb der Uni-Klinik Düsseldorf nach einem Angriff praktisch zum Erliegen. Und im Mai 2021 legen Hacker die grösste amerikanische Ölpipeline teilweise lahm. Solche Vorfälle schrecken auf und führen vor Augen, wie wichtig eine umfassende Cyber Defence ist. Mit dem «Minimalstandard zur Verbesserung der IKT-Resilienz» zeigt der Bund, wo in der Schweiz Handlungsbedarf besteht. Die Empfehlungen richten sich insbesondere an die Betreiber von Kritischen Infrastrukturen und dienen als Richtschnur zur Verbesserung der IKT-Resilienz. Wie wir aus unserer Erfahrung wissen, verdient dabei das Supply-Chain-Risiko ein besonderes Augenmerk.

Die eingebaute Gefahr in Hardware- und Software-Komponenten

Fakt ist, dass die Betreiber von Kritischen Infrastrukturen ihre Soft- und Hardware vor allem bei Lieferanten aus den USA und Asien beziehen. Oftmals haben dabei auch die kleinsten Bausteine ein Stück Software eingebaut, damit sie ihre spezifische Funktion erfüllen können. Diese Komponenten können fehlerhaft sein oder manipuliert werden – sogar ohne, dass die Hersteller oder Lieferanten davon wissen. Sobald irgendwo in der Lieferkette eine Sicherheitslücke auftritt, ist sie ein potenzieller Angriffspunkt für Sabotageakte auf Kritische Infrastrukturen. Nach Meinung von Security-Experten könnten sogar nationale Interessen von Staaten hinter solchen Aktionen stecken. Es wäre naiv

zu glauben, dass Staaten die Möglichkeiten der strategischen Einflussnahme unterhalb der Konfliktschwelle nicht zumindest in Betracht ziehen.

Klar ist: Das Aufspüren bestehender Schwachstellen gleicht der Suche nach der Nadel im Heuhaufen. Betreiber von Kritischen Infrastrukturen tun darum gut daran, ihre Lieferanten punkto Lieferketten-Management in die Pflicht nehmen, damit sie ihre jeweilige Supply Chain systematisch auf allfällige Manipulationen untersuchen. Hilfreich dabei sind unabhängige Experten-Organisationen mit spezialisiertem Fachwissen, die solche Tests durchführen und die Resultate interpretieren können.

Je vernetzter, desto anfälliger

Dass sich die Gefahr zuspitzt, hat nicht nur damit zu tun, dass es für Betreiber von Kritischen Infrastrukturen immer aufwändiger wird, sämtliche Risiken in der verästelten Supply Chain aufzuspüren. Sondern auch damit, dass die zunehmende Digitalisierung und Vernetzung eine zusätzliche Bedrohung darstellen. Bis anhin waren viele Systeme im Bereich Kritischer Infrastrukturen in eine proprietäre Protokolllandschaft eingebunden. Somit waren sie nicht automatisch mit dem Internet oder untereinander verknüpft. Doch das hat sich geändert: Durch die automatisierten Prozesse, die Einbindung von Lieferanten in die Supply Chain und prozessübergreifende Vernetzung werden Brücken vom Internet ins Kontrollsystem geschaffen. Das Beispiel der Stromversorgung zeigt: Das Smart Grid wird von digitalen Technologien durchdrungen – etwa digitalen Mess-, Monitoring- und Steuerungssysteme oder Anwendungen des Internet of Things (IoT). Solche Online-Schnittstellen machen das System verwundbar, weil Schwachstellen aus der Ferne aufgespürt und ausgenutzt werden können.

Dazu kommt: Während IT-Anwendungen tendenziell nach kurzer Zeit aufdatiert oder erneuert werden, finden sich in vielen Kritischen Infrastrukturen Systeme mit langen Lebenszyklen. Diese – aus IT-Sicht uralten – Systeme wie beispielsweise Windows XP oder 7 werden von Herstellern nicht mehr gepflegt und sind nicht für heutige Cyber-Bedrohungen ausgelegt. Dies führt dazu, dass Systeme auch für bereits bekannte Bedrohungen (z.B. Malware) anfällig sind, da keine aktuellen Sicherheitspatches eingespielt werden. Weiter kann es zudem vorkommen, dass Betreiber von Kritischen Infrastrukturen aufgrund einer Beschränkung des Speicherplatzes dazu gezwungen werden, Daten auf externen Server im Intranet abzulegen. Dafür werden von älteren Systemen lediglich Protokolle ohne Sicherheitsfunktionen (wie ftp, vnc, telnet, http) zur Verfügung gestellt. Somit entsteht eine bekannte und für Cyber-Kriminelle einfach zu nutzende Schwachstelle.

Verschiedene Angriffsszenarien

Solche Schwachstellen gibt es viele. Und sie sind nicht in allen Sektoren gleich. Wie die Grafik von PwC zeigt, muss sich beispielsweise ein Elektrizitätswerk auf andere Angriffe einstellen als ein Spital. Im Gesundheitswesen überwiegen Erpressungsversuche mittels Ransomware und Datendiebstahl (Breach). Ganz anders das Bild bei der Stromversorgung: Angriffe auf Energieunternehmen geschehen mit der Absicht, möglichst grosse Anlagenteile zu infizieren und den Betrieb für längere Zeit lahmzulegen (Malware-Attacke) – mit entsprechend schwerwiegenden Folgen für die Versorgung der Bevölkerung mit essenziellen Gütern und Dienstleistungen.

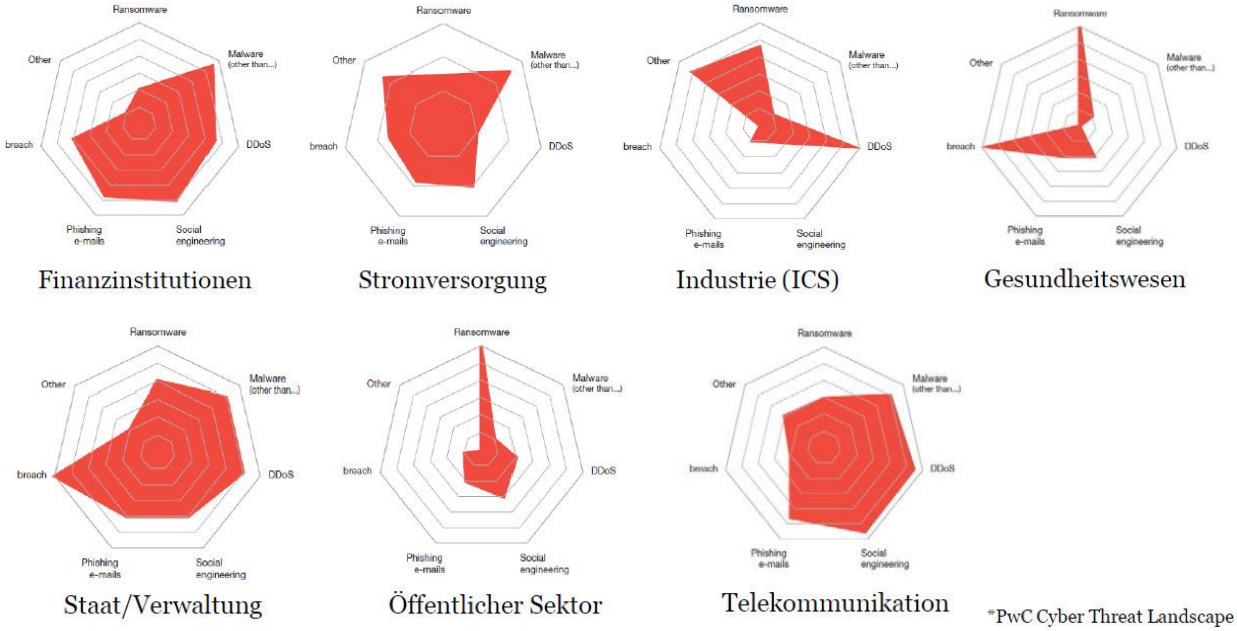

Abbildung 1: Bedrohungslage der verschiedenen KI-Sektoren
Quelle: PwC Cyber Threat Landscape, PwC Digital Services

Für die Entwicklung von Sensibilisierungs- und Schutzmassnahmen sind solche Erkenntnisse hilfreich. Denn sie geben nicht nur Aufschluss über Angriffsziele, sondern auch über die Motivation der Täter. Bei Kritischen Infrastrukturen ist das Schadenspotenzial wesentlich höher als bei anderen Unternehmen, denn die Auswirkungen eines Angriffs betreffen nicht nur eine Organisation, sondern potenziell die gesamte Bevölkerung. Das kann das reibungslose Funktion eines Staates gefährden. Deshalb gerät dieser Bereich nicht nur ins Visier finanziell motivierter Täter, sondern ist auch für Täter mit politischer Motivation oder für staatliche Akteure attraktiv. Die Bereiche Staat und Verwaltung liegen per se im Angriffsspektrum dieser Tätergruppen.

Minimalstandards sind wenig verpflichtend

Vor dem Hintergrund dieser Gefahren sollte dem Schutz Kritischer Infrastrukturen hohe Priorität eingeräumt werden. Der spezielle Fokus auf Supply Chain-Security ist dabei ein Muss. Die vom Bund entwickelten Minimalstandards sind sicher ein wichtiger und guter Anfang. Doch auch die Betreiber von Kritischen Infrastrukturen stehen in der Verantwortung: Sie müssen selber aktiv werden und eine verbindliche Security-Strategie für sich festlegen – am besten basierend auf anerkannten Standards wie beispielsweise die IEC 62443. Das hat drei Vorteile:

1. Ein anerkannter Standard ermöglicht, den eigenen Handlungsbedarf neutral zu eruieren, allfällige Massnahmen risikobasiert und wirtschaftlich zu definieren und Risiken schrittweise abzumildern.
2. Betreiber von Kritischen Infrastrukturen können dank standardisierter Vorgaben ihre eignen Fortschritte regelmässig überprüfen und die nächsten Schritte in Form einer Sicherheits-Roadmap festlegen – sowie gegenüber den Behörden und weiteren Stakeholdern kommunizieren.
3. Schliesslich hilft ein Standard auch dabei, konkrete Anforderungen hinsichtlich Cyber- und IoT-Security zu formulieren und von Herstellern von IoT-Anwendungen von Beginn weg einzufordern.

Solche Standards unterstützen auch Behörden bei der adäquaten Einschätzung der Gefahrenlage in den verschiedenen Sektoren. Schweizer Hersteller leisten hier einen wertvollen Beitrag und sollen dabei zusammenarbeiten – schliesslich steht die Versorgungssicherheit der Schweiz auf dem Spiel.

CyOne Security – der vertrauensvolle Partner von Kritischen Infrastrukturen

Es gilt also, die Kritischen Infrastrukturen in der Schweiz vor Cyber-Risiken zu schützen. Denn moderne und sichere Kritische Infrastrukturen bilden das Rückgrat von Staat und Wirtschaft und sind unabdingbar. Eine sicherheitsverifizierte Supply Chain garantiert die Verfügbarkeit essenzieller Dienstleistungen und trägt so entscheidend zum nachhaltigen Erfolg, zur Wettbewerbsfähigkeit und zur Versorgungssicherheit der Schweiz bei.

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bietet die CyOne Security AG den kundenspezifischen Cyber-Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für die Sicherheitsverifikationen von Produkten, Systemen sowie Operational Security an.

Beginnen Sie heute, Ihre Kritische Infrastruktur und somit die Schweiz vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.