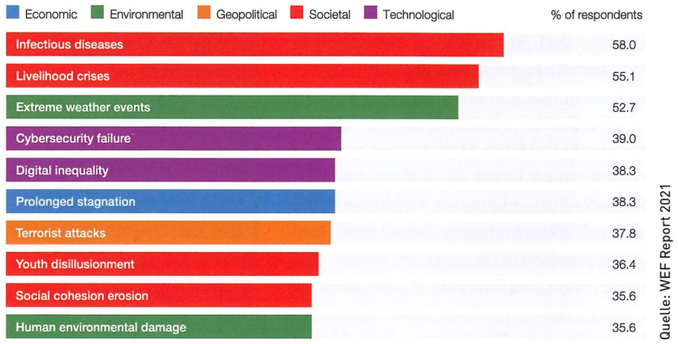
Infrastrukturen: Reaktive Verteidigung reicht nicht aus

Wir leben im digitalisierten Zeitalter, in dem Menschen, Kommunikationsmittel, Fahrzeuge, Maschinen, industrielle Steuerungen über Datennetzwerke verbunden sind. Datenaustausch und Vernetzung gehen heute weit über Geräte hinaus, welche man auf den ersten Blick als digital oder computergestützt wahrnimmt, und durchdringen den physischen Raum zunehmend.

Mischa Obrecht, Jacek Jonczy

Durch das digitale Zeitalter ergeben sich immer stärker werdende Wechselwirkungen beziehungsweise ein Auswirkungspotenzial von Vorfällen im digitalen, d.h. Cyberraum auf die physikalische Wirklichkeit.

Clear and present dangers
Short-term risks (0 – 2 years)



Quelle: WEF Report 2021

Abb. 1: Cyberangriffe gehören zu den globalen Toprisiken.

Cyberangriffe sind ein globales Toprisiko

Cyberkriminelle und staatliche Akteure sind in der Lage, Schwachstellen im Cyberraum auszunutzen, um Wirkung in der physischen Welt zu erzielen, und tun dies auch zunehmend. Das ist ein globales Phänomen und betrifft alle Branchen und Nationen. Im Zusammenhang mit kritischer Infrastruktur wie Industriesteuerungen (Operational Technology – OT) in der Energieversorgung, medizinische Geräte in Spitälern oder Logistik und Transport geht es dabei schnell um Leib und Leben. Dies widerspiegelt sich im globalen Risk Report des WEF (siehe Abb. 1), welcher jährlich publiziert wird und in welchem Cyberangriffe schon länger zu den globalen Toprisiken gehören.

Digitalisierung ist ein Erfolgsfaktor für Cyberangriffe

Die Digitalisierung verstärkt jegliche Skaleneffekte durch Beschleunigung von Prozessen und erhöhter Vernetzung und wird so paradoxerweise auch zum «Enabler» für Cyberangriffe. Der Wert von Informationen und Informationssystemen für Unternehmen und Gesellschaft nimmt zu, Vertraulichkeit, Verfügbarkeit und Korrektheit von Informationen ist in vielen Fällen überlebenswichtig. Potenzielle Zielsysteme und -personen sind auf allen digitalen Kanälen wie Mobile, Home Entertainment, Remote Work, Gebäudeautomatisierung usw. erreichbar und vereinfachen somit auch den Zugang für Angreifer. Verteilte Bezahlsysteme wie Bitcoin oder Monero bzw. Kryptowährungen bieten gewisse Anonymität und dadurch Schutz für Kriminelle und vereinfachen die Bezahlung von Lösegeldforderungen im Zusammenhang mit Erpressungen massiv.

Angreifer und Verteidiger befinden sich nicht im Kräftegleichgewicht

Aufgrund der Anonymität des Internets sowie fehlender internationaler Zusammenarbeit in der Strafverfolgung sind illegale und/oder bösartige Aktivitäten mit minimalem Risiko verbunden.

Es liegt ausserdem in der Natur von Hard- und Softwaresystemen, dass diese Implementierungsfehler aufweisen, welche unter Umständen ausgenutzt werden können. Diese Schwachstellen rechtzeitig zu identifizieren und auszubessern («patchen») ist – insbesondere in stark regulierten Umfeldern – eine grosse organisatorische Herausforderung, da das Risiko von unerwünschten Nebeneffekten besteht. Die Gesamtheit aller Schwachstellen stellt die sogenannte Angriffsfläche einer Organisation dar. Für einen Angreifer reicht es oft aus, eine einzige geeignete Schwachstelle zu finden und auszunutzen. Digitalisierung sei Dank geschieht dies automatisiert und in enormem Tempo. Ausserdem müssen sich Angreifer in den meisten Fällen nicht um unerwünschte Nebenwirkungen ihrer Aktivitäten sorgen. Die Verteidiger müssen mit diesem Tempo Schritt halten und stets den Überblick behalten.

All dies führt zu einem globalen Ungleichgewicht zwischen Angreifer und Verteidiger – zugunsten der Angreifer.

Status quo der Cyberabwehr: Cyberraumbezogene Verteidigung reicht nicht aus

Cyberabwehr beschränkt sich heute im Wesentlichen auf die Cyberdimension. Es werden technologische Lösungen wie Anti-Malware, Firewalls und Netzwerk-

monitoring sowie organisatorische Massnahmen wie Awareness-Kampagnen oder das Patchen von Sicherheitslücken eingesetzt (Vulnerability Management). Wenn im Netzwerk oder auf Rechnern verdächtige Aktivitäten identifiziert und alarmiert werden, ist a priori meist unklar, ob es sich dabei um einen tatsächlichen Sicherheitsvorfall handelt. Häufig handelt es sich bei diesen Alarmen nämlich um Fehlalarme. Wird der Alarm aber als Sicherheitsvorfall bestätigt, erfolgt anschliessend die Bewältigung im Rahmen einer sogenannten Incident-Response. Die zuständigen Analysten sind häufig mit einer Flut wiederkehrender Alarme und Vorfälle konfrontiert, was das Absichern von Systemen und Organisationen sowie die Bewältigung von Sicherheitsvorfällen zu einer äusserst ressourcenintensiven Angelegenheit macht.

Einzelne Vorfälle werden darüber hinaus häufig nicht als kritisch eingestuft. Man denke hier an kritische Infrastruktur wie in der Stromproduktion: Ein physischer Alarm (z.B. ausgelöst durch Sensor oder Kamera am Gebäudeperimeter), eine verdächtige Aktivität im OT-Netzwerk eines Unterwerks oder ungewöhnliche Kommunikation zu einer externen IP-Adresse führen, isoliert betrachtet, möglicherweise nicht zu einem Sicherheitsvorfall. Zeitlich und geografisch korreliert, können diese Alarme jedoch sehr wohl auf einen kritischen Vorfall hindeuten, da es sich möglicherweise um einen Sabotageakt handelt.

All dies führt letztlich dazu, dass sowohl die Genauigkeit in der Detektion von potenziellen Sicherheitsvorfällen als auch die Geschwindigkeit bei deren Bewältigung nicht ausreichen, um mit den Angreifern mitzuhalten. Es ändert sich somit wenig am grundsätzlichen Ungleichgewicht zwischen Angreifer und Verteidiger.

Cybersicherheit – Holistische Sicht ist gefragt

Um ein Kräftegleichgewicht herzustellen bzw. das Ungleichgewicht zwischen Angreifer und Verteidiger im Idealfall umzudrehen, ist eine umfassende Sicht erforderlich. Dazu bieten sich eine Reihe von Massnahmen an: Ansätze für digitale Stolperdrähte und Täuschung des Angreifers (Deception) haben zum Ziel, mit an Sicherheit grenzender Wahrscheinlichkeit schadhafte Aktivitäten zu identifizieren und damit das Problem der Fehlalarme zu entschärfen. Solche Lösungen sind darauf ausgelegt, dass für keinen normalen Benutzer ein Grund besteht, mit dem Stolperdrahtsystem zu interagieren. Für einen ins Netzwerk eingedrungenen Angreifer ist es jedoch schwierig, solche Systeme zu erkennen, und es besteht somit ein relativ hohes Risiko für den Angreifer, mit einem Stolperdrahtsystem zu interagieren und sich damit bemerkbar zu machen.

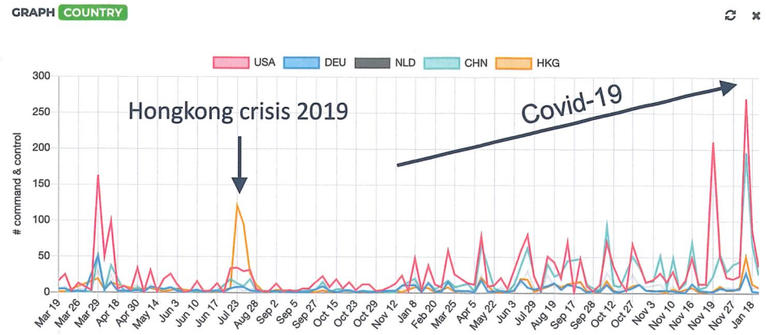


Abb. 2: Threat Intelligence am Beispiel von RATspotting.ch.

Ein weiterer Ansatz ist die Verbesserung der Detektionsgenauigkeit und der Geschwindigkeit in der Erkennung und Bewältigung von potenziellen Vorfällen. Hierfür bietet sich das Teilen von strukturierten Informationen zu neuen Bedrohungen (Threat Intelligence – vgl. Abb. 2), die Automatisierung und Orchestrierung der Bewältigung sowie Korrelation und Kontextualisierung der physischen und der Cyberdimension an: Zusätzlich zu klassischer IT-Infrastruktur müssen die entsprechende physische Ebene sowie andere technische Ebenen (z.B. Operational Technology) berücksichtigt werden. Betroffene Systeme müssen untereinander in Beziehung gebracht und Ereignisse aus unterschiedlichen Domänen miteinander korreliert werden (cross-domain correlation).

Die zunehmende Digitalisierung der physischen Welt kann für die Verbesserung der Detektion so auch einen Nutzen stiften. Zum Beispiel ist ein Ereignis, bei welchem sich ein Benutzer an einer Workstation einloggt und sich gewisse Dateien anschaut, nicht sonderlich verdächtig. Ist aber das entsprechende Detektionssystem mit der Gebäudeautomation vernetzt, entsteht der nötige Kontext: Die Information, dass sich der Benutzer nicht im Gebäude befindet, korreliert mit seinen Aktivitäten an der Workstation, beide sind in Kombination verdächtig und führen zu einem Sicherheitsvorfall. Wir reden in diesem Fall von cyberphysischem Monitoring.

Fazit

Die angesprochenen holistischen Ansätze erfordern das Sammeln und Korrelieren von grossen, potenziell sensitiven Datenmengen. Dies stellt uns vor eine Reihe von Herausforderungen, die es zu adressieren gilt: Technologie (Beherrschen der Datenflut), Organisation (Integration der Techniken in die eigenen Umgebungen und Prozesse) sowie Datenschutz (sensitive Daten müssen entsprechend geschützt sein).

Auch wenn es viel zu tun gibt, sind Lösungsansätze in Sicht. Ein Beispiel, welches fast alle Aspekte adressiert, ist das Horizon-2020-Projekt «Sharing and Automation for Privacy Preserving Attack Neutralization», kurz SAPPAN, in welchem Dreamlab aktiv mitwirkt. ■

MISCHA OBRECHT
Cyber Security Specialist bei Dreamlab Technologies AG
JACEK JONCZY, PHD
Head of Cyber Security Audit & Projects bei Dreamlab Technologies AG

Infrastrukturen: Reaktive Verteidigung reicht nicht aus

Wir leben im digitalisierten Zeitalter, in dem Menschen, Kommunikationsmittel, Fahrzeuge, Maschinen, industrielle Steuerungen über Datennetzwerke verbunden sind. Datenaustausch und Vernetzung gehen heute weit über Geräte hinaus, welche man auf den ersten Blick als digital oder computergestützt wahrnimmt, und durchdringen den physischen Raum zunehmend.

Mischa Obrecht, Jacek Jonczy

Durch das digitale Zeitalter ergeben sich immer stärker werdende Wechselwirkungen beziehungsweise ein Auswirkungspotenzial von Vorfällen im digitalen, d.h. Cyberraum auf die physikalische Wirklichkeit.

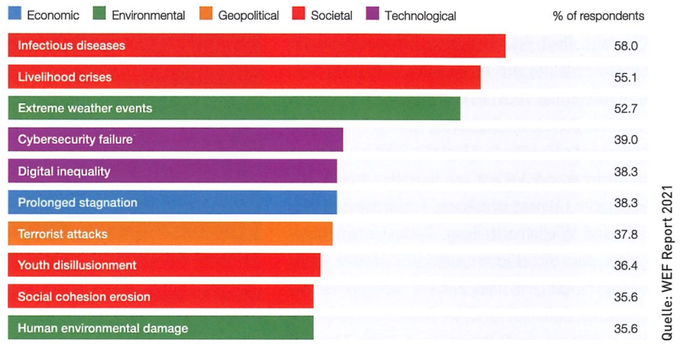


Abb. 1: Cyberangriffe gehören zu den globalen Toprisiken.

Cyberangriffe sind ein globales Toprisiko

Cyberkriminelle und staatliche Akteure sind in der Lage, Schwachstellen im Cyberraum auszunutzen, um Wirkung in der physischen Welt zu erzielen, und tun dies auch zunehmend. Das ist ein globales Phänomen und betrifft alle Branchen und Nationen. Im Zusammenhang mit kritischer Infrastruktur wie Industriesteuerungen (Operational Technology – OT) in der Energieversorgung, medizinische Geräte in Spitälern oder Logistik und Transport geht es dabei schnell um Leib und Leben. Dies widerspiegelt sich im globalen Risk Report des WEF (siehe Abb. 1), welcher jährlich publiziert wird und in welchem Cyberangriffe schon länger zu den globalen Toprisiken gehören.

Digitalisierung ist ein Erfolgsfaktor für Cyberangriffe

Die Digitalisierung verstärkt jegliche Skaleneffekte durch Beschleunigung von Prozessen und erhöhter Vernetzung und wird so paradoxerweise auch zum «Enabler» für Cyberangriffe. Der Wert von Informationen und Informationssystemen für Unternehmen und Gesellschaft nimmt zu, Vertraulichkeit, Verfügbarkeit und Korrektheit von Informationen ist in vielen Fällen überlebenswichtig. Potenzielle Zielsysteme und -personen sind auf allen digitalen Kanälen wie Mobile, Home Entertainment, Remote Work, Gebäudeautomatisierung usw. erreichbar und vereinfachen somit auch den Zugang für Angreifer. Verteilte Bezahlsysteme wie Bitcoin oder Monero bzw. Kryptowährungen bieten gewisse Anonymität und dadurch Schutz für Kriminelle und vereinfachen die Bezahlung von Lösegeldforderungen im Zusammenhang mit Erpressungen massiv.

Angreifer und Verteidiger befinden sich nicht im Kräftegleichgewicht

Aufgrund der Anonymität des Internets sowie fehlender internationaler Zusammenarbeit in der Strafverfolgung sind illegale und/oder bösartige Aktivitäten mit minimalem Risiko verbunden.

Es liegt ausserdem in der Natur von Hard- und Softwaresystemen, dass diese Implementierungsfehler aufweisen, welche unter Umständen ausgenutzt werden können. Diese Schwachstellen rechtzeitig zu identifizieren und auszubessern («patchen») ist – insbesondere in stark regulierten Umfeldern – eine grosse organisatorische Herausforderung, da das Risiko von unerwünschten Nebeneffekten besteht. Die Gesamtheit aller Schwachstellen stellt die sogenannte Angriffsfläche einer Organisation dar. Für einen Angreifer reicht es oft aus, eine einzige geeignete Schwachstelle zu finden und auszunutzen. Digitalisierung sei Dank geschieht dies automatisiert und in enormem Tempo. Ausserdem müssen sich Angreifer in den meisten Fällen nicht um unerwünschte Nebenwirkungen ihrer Aktivitäten sorgen. Die Verteidiger müssen mit diesem Tempo Schritt halten und stets den Überblick behalten.

All dies führt zu einem globalen Ungleichgewicht zwischen Angreifer und Verteidiger – zugunsten der Angreifer.

Status quo der Cyberabwehr: Cyberraumbezogene Verteidigung reicht nicht aus

Cyberabwehr beschränkt sich heute im Wesentlichen auf die Cyberdimension. Es werden technologische Lösungen wie Anti-Malware, Firewalls und Netzwerk-

monitoring sowie organisatorische Massnahmen wie Awareness-Kampagnen oder das Patchen von Sicherheitslücken eingesetzt (Vulnerability Management). Wenn im Netzwerk oder auf Rechnern verdächtige Aktivitäten identifiziert und alarmiert werden, ist a priori meist unklar, ob es sich dabei um einen tatsächlichen Sicherheitsvorfall handelt. Häufig handelt es sich bei diesen Alarmen nämlich um Fehlalarme. Wird der Alarm aber als Sicherheitsvorfall bestätigt, erfolgt anschliessend die Bewältigung im Rahmen einer sogenannten Incident-Response. Die zuständigen Analysten sind häufig mit einer Flut wiederkehrender Alarme und Vorfälle konfrontiert, was das Absichern von Systemen und Organisationen sowie die Bewältigung von Sicherheitsvorfällen zu einer äusserst ressourcenintensiven Angelegenheit macht.

Einzelne Vorfälle werden darüber hinaus häufig nicht als kritisch eingestuft. Man denke hier an kritische Infrastruktur wie in der Stromproduktion: Ein physischer Alarm (z.B. ausgelöst durch Sensor oder Kamera am Gebäudeperimeter), eine verdächtige Aktivität im OT-Netzwerk eines Unterwerks oder ungewöhnliche Kommunikation zu einer externen IP-Adresse führen, isoliert betrachtet, möglicherweise nicht zu einem Sicherheitsvorfall. Zeitlich und geografisch korreliert, können diese Alarme jedoch sehr wohl auf einen kritischen Vorfall hindeuten, da es sich möglicherweise um einen Sabotageakt handelt.

All dies führt letztlich dazu, dass sowohl die Genauigkeit in der Detektion von potenziellen Sicherheitsvorfällen als auch die Geschwindigkeit bei deren Bewältigung nicht ausreichen, um mit den Angreifern mitzuhalten. Es ändert sich somit wenig am grundsätzlichen Ungleichgewicht zwischen Angreifer und Verteidiger.

Cybersicherheit – Holistische Sicht ist gefragt

Um ein Kräftegleichgewicht herzustellen bzw. das Ungleichgewicht zwischen Angreifer und Verteidiger im Idealfall umzudrehen, ist eine umfassende Sicht erforderlich. Dazu bieten sich eine Reihe von Massnahmen an: Ansätze für digitale Stolperdrähte und Täuschung des Angreifers (Deception) haben zum Ziel, mit an Sicherheit grenzender Wahrscheinlichkeit schadhafte Aktivitäten zu identifizieren und damit das Problem der Fehlalarme zu entschärfen. Solche Lösungen sind darauf ausgelegt, dass für keinen normalen Benutzer ein Grund besteht, mit dem Stolperdrahtsystem zu interagieren. Für einen ins Netzwerk eingedrungenen Angreifer ist es jedoch schwierig, solche Systeme zu erkennen, und es besteht somit ein relativ hohes Risiko für den Angreifer, mit einem Stolperdrahtsystem zu interagieren und sich damit bemerkbar zu machen.

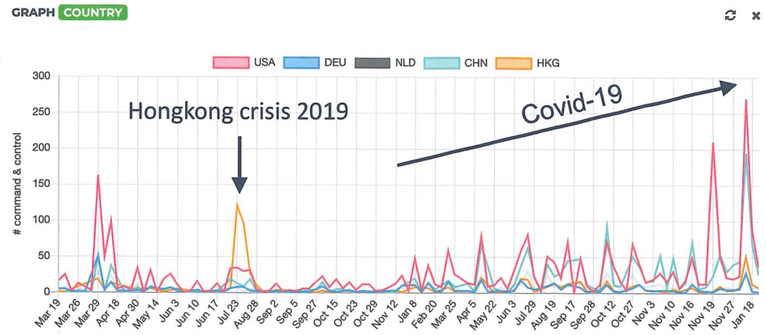


Abb. 2: Threat Intelligence am Beispiel von RATspotting.ch.

Ein weiterer Ansatz ist die Verbesserung der Detektionsgenauigkeit und der Geschwindigkeit in der Erkennung und Bewältigung von potenziellen Vorfällen. Hierfür bietet sich das Teilen von strukturierten Informationen zu neuen Bedrohungen (Threat Intelligence – vgl. Abb. 2), die Automatisierung und Orchestrierung der Bewältigung sowie Korrelation und Kontextualisierung der physischen und der Cyberdimension an: Zusätzlich zu klassischer IT-Infrastruktur müssen die entsprechende physische Ebene sowie andere technische Ebenen (z.B. Operational Technology) berücksichtigt werden. Betroffene Systeme müssen untereinander in Beziehung gebracht und Ereignisse aus unterschiedlichen Domänen miteinander korreliert werden (cross-domain correlation).

Die zunehmende Digitalisierung der physischen Welt kann für die Verbesserung der Detektion so auch einen Nutzen stiften. Zum Beispiel ist ein Ereignis, bei welchem sich ein Benutzer an einer Workstation einloggt und sich gewisse Dateien anschaut, nicht sonderlich verdächtig. Ist aber das entsprechende Detektionssystem mit der Gebäudeautomation vernetzt, entsteht der nötige Kontext: Die Information, dass sich der Benutzer nicht im Gebäude befindet, korreliert mit seinen Aktivitäten an der Workstation, beide sind in Kombination verdächtig und führen zu einem Sicherheitsvorfall. Wir reden in diesem Fall von cyberphysischem Monitoring.

Fazit

Die angesprochenen holistischen Ansätze erfordern das Sammeln und Korrelieren von grossen, potenziell sensitiven Datenmengen. Dies stellt uns vor eine Reihe von Herausforderungen, die es zu adressieren gilt: Technologie (Beherrschen der Datenflut), Organisation (Integration der Techniken in die eigenen Umgebungen und Prozesse) sowie Datenschutz (sensitive Daten müssen entsprechend geschützt sein).

Auch wenn es viel zu tun gibt, sind Lösungsansätze in Sicht. Ein Beispiel, welches fast alle Aspekte adressiert, ist das Horizon-2020-Projekt «Sharing and Automation for Privacy Preserving Attack Neutralization», kurz SAPPAN, in welchem Dreamlab aktiv mitwirkt. ■

MISCHA OBRECHT
Cyber Security Specialist bei Dreamlab Technologies AG
JACEK JONCZY, PHD
Head of Cyber Security Audit & Projects bei Dreamlab Technologies AG