Kann es Cybersicherheit wirklich geben?

Kann es Cybersicherheit wirklich geben?

Das Thema Cybersecurity beherrscht unsere Gesellschaft. Seien es nun die Cyberkriminellen, die mit ihren Ransomware-Angriffen die Privatwirtschaft plagen. Oder die technischen Konsequenzen, die gewisse geopolitische Stossrichtungen mit sich bringen. Bei all der Diskussion verliert man sich schnell in den Details.

Marc Ruef

Im Duden findet sich eine treffende Bedeutung des Worts «Sicherheit», die da lautet: «Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden; höchstmögliches Freisein von Gefährdungen». Obwohl diese Definition mit hoher Wahrscheinlichkeit nicht mit Rücksicht auf das Thema «Cybersicherheit» ausgearbeitet wurde, vermag die unverbindliche Zusammenfassung auch diese mitzuberücksichtigen. Ist Sicherheit aber in Bezug auf Cyber möglich und umsetzbar?

Ein System ist dann sicher, wenn es seine Aufgabe erledigt, ohne ausserhalb des definierten Rahmens zu agieren. Wenn ein Computer also eine Addition der Form (x + y) durchzuführen hat und auch nur dies kann, dann ist er per Definition sicher (sofern natürlich die Aufgabe an sich keine Unsicherheit darstellt). Wir können weiter davon ausgehen, dass ein Computersystem eine endliche Anzahl Zustände hat und dementsprechend deterministisch ist. Wenn all diese Zustände auf ihre Richtigkeit hin geprüft und diese durchgesetzt werden kann, dann ist es als sicher anzusehen. Also eigentlich eine einfache Angelegenheit. Jedoch leider nur auf dem Papier.

Komplexität als Feind Nummer Eins

Die Anzahl der Zustände eines Computersystems mögen endlich sein. Doch diese Anzahl ist unglaublich gross. Jede einzelne Hardware-Komponente ist ein Mikrokosmos, der viele Zustände mitbringt. Die Kombination dieser gepaart mit den individuellen Möglichkeiten der Software-Programmierung erzeugen eine Komplexität, die in der Realität nur noch wenig mit Endlichkeit zu tun hat.

Es bleibt somit theoretisch möglich, dass auf dem Papier die Zustände analysiert und als «sicher» identifiziert werden können. Eine solche Analyse dauert aber dermassen lange und ist mit derlei vielen Fehlerquellen behaftet, dass halt eben doch keine abschliessende Bewertung erfolgen kann. Vor allem keine, die sich in wirtschaftlicher Weise irgendwie rechtfertigen liesse. Welche Organisation ist bereit, Millionen für die Sicherheitsanalyse eines primitiv erscheinenden Arbeitsplatzrechners aufzuwenden? Oder eines Servers mit Datenbank und Webapplikation? Und hätte man diese Investition getätigt, müsste sie von vorne beginnen, sobald eine Einstellung angepasst, eine Komponente ausgetauscht oder eine Software aktualisiert wurde. Eine Sisyphusarbeit, die ihres Gleichen suchen würde. Das will niemand, das kann niemand, das macht niemand.

Das unbekannte Wesen

Bisher gingen wir stets davon aus, dass wir wissen, was wir tun. Im Beispiel wird eine Addition als (x + y) eingebracht. Eine simple Angelegenheit. Doch auch hier eröffnen sich Schwierigkeiten, die man nicht erwarten würde. Der Speicher von Computersystemen ist naturbedingt begrenzt. Das Berechnen der Summe (1 + 2) ist in der Regel ein Kinderspiel. Was aber, wenn plötzlich mit Zahlen gerechnet wird, die den verfügbaren Speicherplatz sprengen? Speicherschutzverletzungen sind die Folge davon. Das gezielte Überschreiben von Speicherbereichen erlaubt das Verändern des Programmverhaltens. Eine klassische Schwachstelle namens Pufferüberlauf, die Mitte der 1990er Jahre durch Angreifer kultiviert wurde und auch heute noch so manches System zu erschüttern vermag.

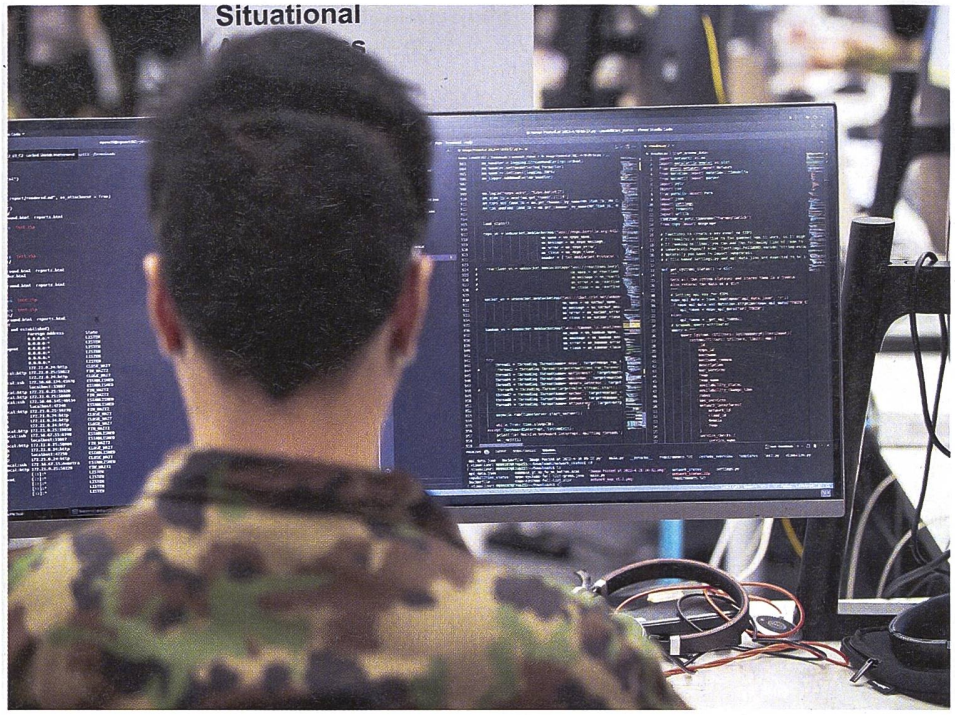
Damit sind die Möglichkeiten aber noch nicht erschöpft. Was passiert, wenn y nicht eine positive, sondern eine negative Zahl ist? Es wird dann 1 mit -2 addiert, was zum negativen Wert -1 führt. Je nachdem ist die Software oder die Hardware nicht darauf ausgelegt, ein negatives Resultat abzulegen. Dies kann wiederum zu einem unerwarteten Zustand führen. Es gibt verschiedene Varianten dieser Angriffstechnik, die als Integer Underflow oder Wraparound bezeichnet wird. Eine dermassen geringfügige Anomalie kann verheerende Folgen für die Sicherheit eines Systems haben.

Der Gedanke kann weitergeführt werden. Was passiert, wenn Dezimalzahlen mit Nachkommastellen, Buchstaben, Sonderzeichen oder Zeichen aus einem fremden Zeichensatz verwendet werden? Eine Spielwiese für Angreifer. Und glauben Sie mir, die tummeln sich gerne auf dieser! Grundsätzlich ist es die Aufgabe des Entwicklers, solche Sonderfälle abzufangen. Lange und grosse Eingaben müssen beispielsweise geprüft werden, um sie bei problematischen Strukturen normalisieren oder verwerfen zu können. Die genannten Beispiele sind nur die Spitze des Eisbergs. Es gibt Dutzende verschiedener Angriffstechniken, die ihrerseits eine Vielzahl von Untertechniken, Varianten oder Kombinationen erlauben. Für einen Entwickler ist es nahezu unmöglich all diese Abweichungen kennen, fachgerecht adressieren und korrekt implementieren zu können. Zwar erleichtern moderne Programmiersprachen und verfügbare Frameworks diese Aufgabe, doch sie sind doch nur ein Tropfen auf den heissen Stein.

Hinzu kommt, dass die eingesetzte Hardware und Software immer abstrahierter wurden. Es werden neue Ansätze eingeführt, erweiterte Protokolle etabliert, Algorithmen optimiert, unterschiedliche Encodierungen implementiert, Komponenten virtualisiert und Daten cloudifiziert. Es ist unmöglich, heute noch ein guter Generalist im IT-Bereich zu sein.

Was gilt es zu tun

Keine Panik und Ruhe bewahren. Damit ist die innerliche «Ruhe» gemeint und nicht ein nachlässiges «Ausruhen». Sonst finden einem irgendwann die Ransomware-Gangs, kompromittieren die Umgebung und verhelfen einem zu einer ungewollten Präsenz in den Tagesmedien. Cybersecurity muss ernst genommen werden. Aber möglichst ohne Hektik. Man sollte sich mit den Technologien auseinandersetzen und stetig fragen, ob deren Einsatz gerechtfertigt ist und



◀ **Cybersecurity geht alle an, ob im Militär oder im Zivilen.** Bild: Claudia Christen, VBS

welche Konsequenzen ein solcher einführt. Falls Abhängigkeiten und Komplexitäten das vertretbare Mass übersteigen, sind sie nicht die richtige Wahl. Ein ungutes Bauchgefühl oder gar schlaflose Nächste sind immer ein ganz schlechtes Zeichen. Dann sollte man bewusst einen Schritt zurückgehen und nach alternativen Lösungen suchen. Kommt Zeit, kommt Rat.

Dieses vorausschauende Denken ist unabdingbar, um sich nicht in einer technologischen Abhängigkeit zu verlieren, die sich als faustischer Pakt mit dem Teufel herausstellen wird. Die Schönrederei, mit denen Produkthersteller ihre hübschen Lösungen etablieren wollen, müssen kritisch hinterfragt werden. Nur mit der nötigen Skepsis kann die dringend erforderliche Unabhängigkeit und Flexibilität gewahrt werden. Und die Sicherheit ist ein mehr oder weniger automatisches Beiprodukt dieser intelligenten Entscheidungsfindung. Wie zuvor erklärt, ist es unmöglich, ein System mit absoluter Gewissheit auf seine Sicherheit hin zu prüfen. Geschweige denn ein solches zu entwickeln. Wir müssen mit Unsicherheiten leben. Wir müssen damit zurechtkommen, dass falsche Entscheidungen getroffen werden. Aber wir sollten es nicht akzeptieren, wenn nachweislich Nachlässigkeiten in Kauf genommen und offensichtliche Dummheiten begangen und gar noch zelebriert werden. Verantwortlichkeit ist ein wichtiges Element, um Leute zur Disziplin zu zwingen. Und Disziplin bleibt zum Schluss eine elementare Grundlage von Sicherheit.

Professionalisierung der Cybersicherheit

Cybersecurity ist ein unglaublich breites und vielschichtiges Thema. Mathematik, Physik, Elektronik, Informatik an einem Ende, Psychologie und Soziologie am anderen Ende des Spektrums. Hier mit alleiniger Kraft seinen Meister zu stehen ist schlichtweg nicht mehr möglich. Man muss sich auf das Wissen und die Leistung anderer verlassen können. Dementsprechend ist es keine Schande, bei spezifischen Problemen entsprechende Experten beizuziehen, die mit ihrem Spezialwissen und ihrer Erfahrung das Bestmögliche erarbeiten können.

So manche Organisation behandelt Cybersecurity stiefmütterlich, kommt nur am Rande oder praktisch gar nicht bewusst in Kontakt damit. Diesen sei ans Herz gelegt, dass es Firmen gibt, die den ganzen Tag nur dies machen. Von diesen kann man profitieren. Da muss man vielleicht auch mal das eigene Ego zurückstecken und eingestehen, dass jemand anderes etwas «besser» kann. Diese Art der Demut ist der entscheidende erste Schritt in die Professionalität.

Für Behörden bedeutet dies, dass sie eine nahe und intensive Zusammenarbeit mit der Privatwirtschaft etablieren müssen. Diese ist den Zwängen und dem Druck der Industrie und der Mitbewerber unterworfen, wodurch in der Regel ein Mehr an aktuellem Wissen erarbeitet und gelebt werden muss. Dabei darf man sich nicht von internationalen Firmen mit ihren grossen Namen und den polierten Folien blenden lassen. Wahre Innovation wird nur durch Flexibilität und Agilität möglich, die halt eben nur kleine Unternehmen in diesem Bereich mitbringen können. In der Schweiz gibt es diesbezüglich ein paar Perlen, die die letzten 25 Jahre einen grossartigen Beitrag zur weltweiten Cybersecurity-Community geleistet haben. Leider ist der Prophet im eigenen Land oft mal wenig wert. Man sollte aber auch nicht unnötig in die Ferne schweifen. Die Nähe zum akademischen Bereich hilft dabei, langfristige und anstehende Entwicklungen als solche wahrzunehmen, um sich strategisch richtig positionieren zu können. Und im Idealfall einen wichtigen Schritt voraus zu sein.

Alle sind betroffen

Cybersecurity ist ein Thema, das in den Mittelpunkt des alltäglichen Lebens vorgerückt ist. Es betrifft uns alle, egal ob privat, beruflich oder in der Kaderfunktion in der Armee. Sich vor den Risiken zu verstecken, ist unmöglich, weshalb man sich mit ihnen auseinandersetzen muss. Das grundlegende Verständnis für etablierte Mechanismen und Technologien ist dabei genauso wichtig, wie das Wissen um potenzielle Bedrohungen. Es bleibt uns allen also nichts anderes übrig, als mit offenen Augen den digitalen Bereich im Blick zu behalten.

Risiken können oftmals nicht komplett eliminiert werden. Manchmal muss man sie halt eingehen, das ist Teil des Lebens. Wenn man ein Risiko jedoch eingeht, muss man sich dessen bewusst sein und die Auswirkungen des Eintretens eines Schadens in Kauf nehmen können. Cybersecurity ist nicht einfach. Aber es liegt an jedem Einzelnen, es halt eben möglichst richtig zu machen. ■

Marc Ruef
Head of Research scip AG
8048 Zürich