Das Schweizer Industriemagazin. Seit 1972. www.maschinenbau-schweiz.ch

maschinenbau

Nr. 8 August 2023

MIT MB-SPECIAL ZERSPANUNGSTECHNIK SOWIE EMO- UND SINDEX-VORSCHAU

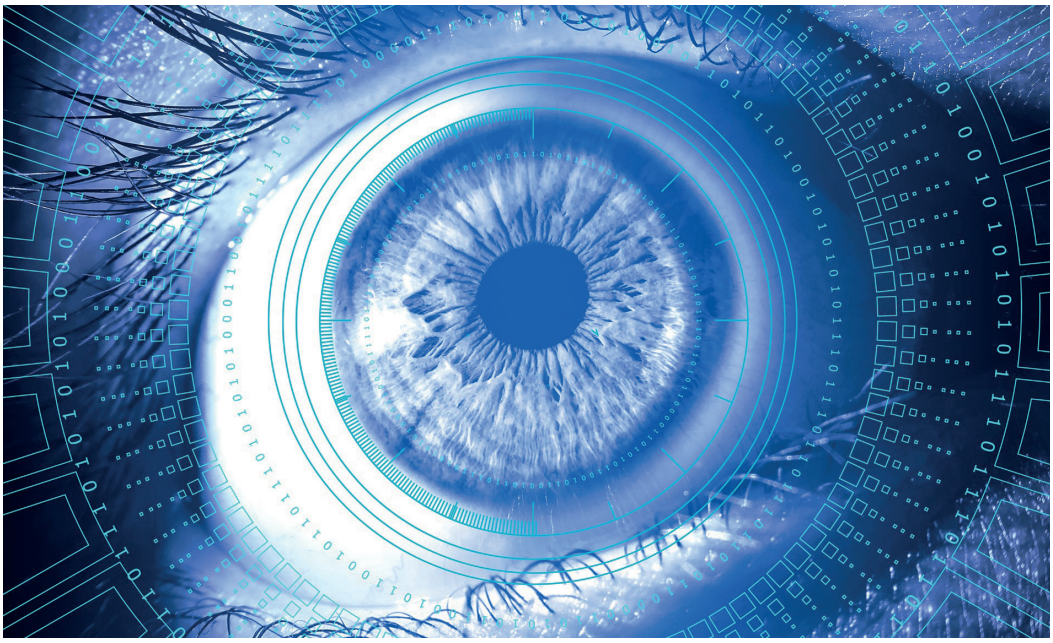

Bild: Pixabay

Cybersicherheit ist von entscheidender Bedeutung für eine funktionierende Sicherheitsstrategie.

Nationale Cyberstrategie des Bundes (NCS)

Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen. Sie gehört zu den weltweit führenden Wissens-, Bildungs- und Innovationsstandorten in der Cybersicherheit. Die Handlungsfähigkeit und die Integrität ihrer Bevölkerung, ihrer Wirtschaft, ihrer Behörden und der in der Schweiz ansässigen internationalen Organisationen gegenüber Cyberbedrohungen sind gewährleistet. Doch wie möchte der Bund diese Vision erreichen? Im April 2023 wurde die neue nationale Cyberstrategie veröffentlicht. Zeit also, genauer in diese zu schauen.

Bereits in der Einleitung wird klar, dass das Thema Cyber-Sicherheit nicht auf zwei, drei Seiten bearbeitet werden kann. Sie ist ein Schlüsselelement für die Informationssicherheit und den Datenschutz, dient als Voraussetzung für die Digitalisierung und ist auch wichtig für die Innen- und Aussenpolitik des Bundes.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Die Strategie versucht die Themen zu sortieren, zu gewichten und in Relation zueinander zu setzen.

Fünf verschiedene Szenarien

Als Cyberbedrohung wird in der Strategie ein Umstand bezeichnet, der das Potenzial hat, einen Cybervorfall zu verursachen. Ein Cybervorfall ist wiederum definiert als Ereignis, das bei der ICT-Nutzung die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt. Dabei wird der Vorfall absichtlich herbeigeführt. Daher werden der Zweck der Angriffe, die Akteure, welche hinter den Angriffen stehen, und die angegriffenen Parteien als Unterscheidungskriterium verwendet. Die Strategie behandelt in der Folge fünf verschiedene Szenarien:

Cyberkriminalität

Damit sind vor allem Vermögensdelikte gemeint, die entweder direkt auf IT-Systeme gerichtet sind (Cybercrime) oder in der analogen Welt vorkommen, die aber vermehrt digitale Werkzeuge mitnutzen (Digitalisierte Kriminalität).

Cyberspionage

Für politische, militärische oder wirtschaftliche Zwecke wird versucht unerlaubt an Informationen zu gelangen oder die Aktivitäten der Opfer zu beobachten. Im Fokus der Angreifer stehen sowohl Unternehmen als auch staatliche, gesellschaftliche oder internationale Institutionen. Hier ist die Schweiz besonders stark im Fokus. Die grosse Gefahr besteht darin, dass die Hacker versuchen, so lange wie möglich unerkannt im Netzwerk zu bleiben. Die Strategie geht davon aus, dass hier eine grosse Gefahr ausgeht, da die Folgen oft erst viel später erkannt werden. Zudem wird das Risiko erhöht, da Regierungen Einfluss auf Hersteller von IKT-Produkten ausüben. Dies erhöht die Wahrscheinlichkeit, dass Sicherheitslücken in Produkten bewusst offengelassen werden.

Cybersabotage

Hier werden bewusst ICT-Mittel manipuliert, ge- oder gar zerstört. Die Motivation dahinter kann sehr unterschiedlich sein. Sie können von Einzeltätern beispielsweise aus ideologischen Überzeugungen oder auf Grund persönlicher Frustration durchgeführt oder von staatlichen Akteuren zur Erreichung politischer oder militärischer Ziele eingesetzt werden.

Cybersubversion

Hier versuchen staatliche, staatsnahe oder politisch motivierte Akteure Cyberangriffe gezielt dafür einsetzen, um das politische System eines anderen Staates zu unterminieren.

Cyberoperationen in bewaffneten Konflikten

Gerade bei Konflikten ist es heute ein beliebtes Werkzeug. Ohne grossen Aufwand kann von irgendwo auf der Welt Schaden angerichtet werden.

Weiter können menschliches Fehlverhalten oder technische Ausfälle zu einem Cybervorfall führen. Solche Ereignisse kommen öfters vor und die ICT-Abteilung ist entsprechend darauf vorbereitet und kann die Auswirkungen dieser Fehler und Ausfälle schnell eingrenzen und beheben. Um dies möglichst klein zu halten, bleibt die Awareness der Mitarbeitenden wichtig.

Technologische, politische und gesellschaftliche Entwicklungen haben grossen Einfluss auf die Bedrohungslage. Diese können sich jederzeit und sehr schnell ändern. Daher gilt es diese ständig im Blick zu haben. Auch die Spannungen beziehungsweise der Druck auf Hersteller, wie wir dies aktuell zwischen Amerika und China erleben, tragen ihren Teil dazu bei. Auch technologi-

sche Weiterentwicklungen gilt es im Auge zu behalten. Dazu gehören beispielsweise die Nutzung der Cloud, Internet of Things (IoT) oder die künstliche Intelligenz.

Organisation

Die ersten beiden Strategien (2012-2017/2018–2022) fokussierten auf den Auf- und Ausbau von Fähigkeiten, Strukturen und Prozessen. Die Umsetzung der Strategien hat die nötigen Grundlagen für eine kohärente Cybersicherheitspolitik der Schweiz geschaffen.

Als Basis für die aktuelle Strategie wurden zudem folgende Elemente einbezogen:

- Strategie Digitale Schweiz
- Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)
- Bericht des Bundesrates über die Sicherheitspolitik der Schweiz
- Gesamtkonzeption Cyber der Schweizer Armee
- Strategie Digitalaussenpolitik

Die Organisation ist in der Schweiz eine grosse Herausforderung. So haben der Bund und die Kantone ihre jeweiligen Cyberorganisationen entwickelt. Auch die Zusammenarbeit zwischen öffentlichen und privaten Akteuren in der Cybersicherheit ist von entscheidender Bedeutung für eine funktionierende Sicherheitsstrategie. In der Strategie werden daher die verschiedenen Organisationen und Zuständigkeiten aufgezeigt.

Als strategische Ziele setzt sich die Strategie die folgenden fünf:

1. Selbstbefähigung (damit sind Beurteilung, aktuelle Entwicklungen berücksichtigen sowie offen informieren)
2. sichere digitale Dienstleistungen und Infrastrukturen
3. wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cybervorfällen
4. effektive Bekämpfung und Strafverfolgung der Cyberkriminalität
5. führende Rolle in der internationalen Zusammenarbeit

Als Zielgruppen adressiert die Strategie die Bevölkerung, die Wirtschaft, kritische Infrastrukturen, Behörden, aber auch internationale Organisationen und Nichtregierungsorganisationen.

Massnahmen

Nachfolgend sind die 17 geplanten Massnahmen kurz zusammengefasst. In Klammern ist jeweils angefügt, auf welches der fünf Ziele sich diese bezieht.

M1 (1): Wie in der Wirtschaft, muss auch auf Bundesebene ausreichend fachspezifisches Personal vorhanden sein. Auch die Grundkompetenz der Bevölkerung trägt zum Erfolg bei. Dies soll durch die bestehenden Bildungs- und Forschungsinstitutionen sichergestellt werden. Auch die beachtliche Start-up-Szene ermöglicht, dass die Forschung in der Schweiz auf einem hohen Niveau ist.

M2 (1): Die Sensibilisierung der Bevölkerung ist ein weiterer Schwerpunkt. Dazu gehört auch, dass Einzelpersonen die Kontrolle über ihre persönlichen Daten behalten und Unternehmen und Organisationen ihre Datenbearbeitungsmethoden transparent machen. Damit wird die Resilienz gegenüber Cyberrisiken gestärkt.

M3 (1): Bedrohungen müssen frühzeitig erkannt werden.

Dazu gehört die Feststellung der Akteure und deren Angriffsvektoren und ausgenutzten Schwachstellen. Diese Bedrohungen werden gewichtet und in das periodisch nachgeführte, operative und strategische Bedrohungsbild integriert.

M4 (1): Weil sich digitale Technologien dynamisch entwickeln, ist dabei wichtig, neue Entwicklungen frühzeitig zu erkennen und deren Auswirkungen auf die Sicherheit zu verstehen. Dabei ist es wichtig, die Abhängigkeiten von Herstellern aus dem Ausland und den damit verbundenen Risiken zu kennen. Dazu wird ein Technologiemonitoring aufgebaut. Auch das neue Nationale Testinstitut für Cybersicherheit (NTC) ist ein wichtiger Baustein dazu.

M5 (2): Essenziell wichtig ist es zu verhindern, dass Schwachstellen entstehen und ausgenutzt werden können. Dazu müssen diese rechtzeitig erkannt und rasch behoben werden. Dabei sollen Schwachstellen erst veröffentlicht werden, wenn Gegenmassnahmen vorhanden sind («Coordinated Vulnerability Disclosure»). Geplante Schwerpunkte sind ethisches Hacking institutionalisieren, koordiniertes Vorgehen bei der Veröffentlichung von Schwachstellen, die Kommunikation zentralisieren sowie die automatisierte Schwachstellenerkennung verbessern.

M6 (2): Das konsequente Umsetzen des Grundschutzes bietet einen hohen Schutz gegen Cyberbedrohungen. Dabei werden internationale Standards berücksichtigt. Auch der IKT-Minimalstandard kann als Werkzeug genutzt werden. Der Bund prüft, ob auch rechtliche Vorgaben gestärkt werden können. Die Pflicht zur Meldung von Cyberangriffen wird bereits im Parlament geprüft.

M7 (2): Auch die Zusammenarbeit zwischen den Behörden wird verbessert. Dazu werden das Informationssicherheitsgesetz innerhalb der Bundesverwaltung umgesetzt, der Informationsaustausch zwischen dem NCSC (Nationales Zentrum für Cybersicherheit) und den Fachämtern gestärkt, die Zusammenarbeit zwischen Bund und Kantonen sowie die Unterstützungsleistungen geklärt.

M8 (3): Cybervorfälle kann es jederzeit geben, daher ist es wichtig, frühzeitig die richtigen Gegenmassnahmen zu identifizieren. Dazu gehören der Aufbau und Betrieb einer entsprechenden Organisation. Dazu braucht es Fachkompetenzen, Analyseinstrumente, eine gut funktionierende Organisation mit klar definierten Entscheidungskompetenzen und eine intensive Zusammenarbeit zwischen allen relevanten Stellen.

M9 (3): Nebst der Reaktion ist auch die genaue Identifikation der Angriffs-Urheber wichtig. Mit diesen Informationen kann das weitere Vorgehen geplant werden. Die Identifizierung gelingt nur, wenn Angriffe rechtzeitig erkannt werden und ihr technischer, operationeller und strategischer Kontext analysiert werden kann.

M10 (3): Die Konsequenzen können gravierend sein. Daher ist ein geeignetes Krisenmanagement auf nationaler Ebene wichtig. Entscheidend für die Bewältigung von Krisen sind ein aktuelles, einheitliches und umfassendes Lagebild, die Definition von effizienten Prozessen zur Entscheidungsfindung und die Festlegung einer Kommunikationsstrategie. Zusätzlich gilt es regelmässig Übungen durchzuführen.

M11 (3): Die Abwehr schützt den Staat, die Wirtschaft und die Bevölkerung. Das Ziel ist der Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Schweizer Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden.

Für die interessierten maschinenbau-Leserinnen und -Leser kann die Strategie unter www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html oder mittels QR-Code heruntergeladen werden.

M12 (4): Die Zusammenarbeit bei der Strafverfolgung stellt den Bund und Kantone vor grosse Herausforderungen. Dazu wird das Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK), weiter ausgebaut. Bei Themen wie der digitalen Forensik wird mit Firmen im Privatsektor zusammengearbeitet.

M13 (4): Mit der Fallübersicht werden die Ereignisse übersichtlich dargestellt. Diese Übersicht ermöglicht später in Echtzeit miteinander die aktuelle Lage zu beurteilen.

M14 (4): Ein zentraler Faktor ist auch die Ausbildung der Strafverfolgungsbehörden. Die Grundausbildung zur Cyberkriminalität findet in den Polizeischulen und am Schweizerischen Polizei-Institut (SPI) statt. Weiter wurde mit der Plattform cyberpie.ch eine Übersichtsplattform zu den relevanten Ausbildungsmöglichkeiten geschaffen. Auch ein Cyber-Wiki wurde bereits aufgebaut und wird erweitert.

M15 (5): Der Bundesrat hat sich zum Ziel gesetzt, die Schweiz und namentlich das internationale Genf als führenden Standort der Digitalisierungs- und Technologiedebatten zu positionieren. Dazu soll ein «Information Sharing and Analysis Centre» (ISAC) aufgebaut werden.

M16 (5): Die Schweiz hat sich zum Ziel gesetzt, sich aktiv für ein offenes, freies und sicheres Internet zu engagieren. Dazu nimmt sie aktiv an UNO-Prozessen teil, beteiligt sich an der Weiterentwicklung und der Umsetzung des Übereinkommens über die Cyberkriminalität («Budapest Konvention») sowie bei der Umsetzung der vertrauensbildenden Massnahmen der OSZE.

M17 (5): Weiter werden Massnahmen ergriffen, um die operative Zusammenarbeit mit internationalen Partnern zu stärken, zu koordinieren und gezielt auszubauen. Die Schweiz tauscht sich deshalb auf operativer und strategischer Ebene in den entsprechenden Fachgremien aber auch direkt mit anderen Staaten zu den Cyberthemen aus.

Diese 17 Massnahmen zeigen ein ehrgeiziges Ziel der Schweiz. Für die Umsetzung ist der Steuerungsausschuss zuständig. Die Finanzierung erfolgt durch die zentralen Akteure (Bund, Kantone und weitere Stellen). Hoffen wir, dass die politischen Widerstände dies nicht verzögern und die Schweiz wirklich zu den führenden Nationen in der Awareness und Bekämpfung von Sicherheitsvorfällen wird.