Profi-Guide	
Branche	
Anlagenbau	●
Chemie	● ● ●
Pharma	● ● ●
Ausrüster	● ● ●
Funktion	
Planer	●
Betreiber	● ● ●
Einkäufer	●
Manager	● ● ●

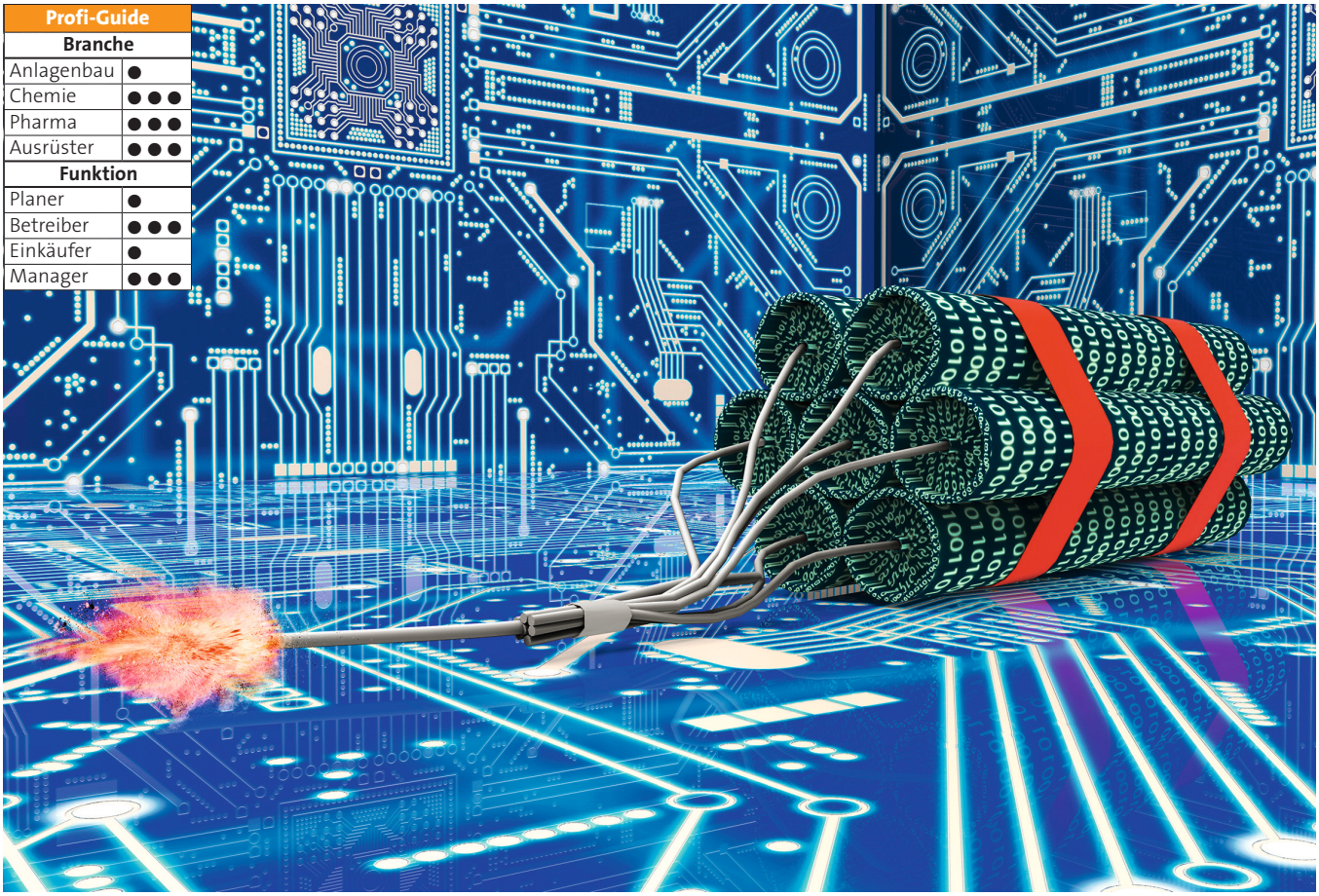


Bild: the_lightwriter – AdobeStock

Furcht vor russischen Cyberangriffen infolge der Unterstützung für die Ukraine

Kollateralschäden in der Industrie befürchtet

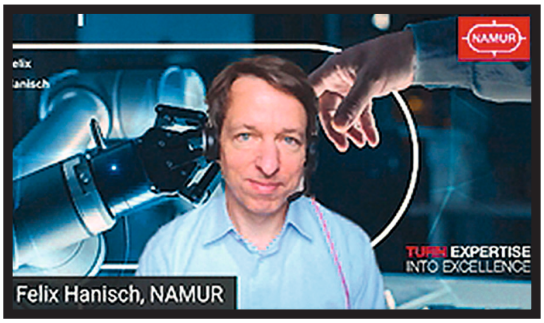
Ransomware-Angriffe auf Pipeline- und Tanklagerbetreiber, Ausfälle bei Windkraftanlagen – immer häufiger geraten Industrieunternehmen in das Fadenkreuz von Hackern. Dabei spielen vor allem in der aktuellen Situation politische Motive eine immer stärkere Rolle, wurde auf den IMI OT-Community Days im Mai deutlich.

An Zufälle glaubt der ehemalige Nato-General Koen Gijsbers in Sachen Cyberattacken schon längst nicht mehr. Ob wiederholte Hackerangriffe auf das noch junge Nato-Mitglied Montenegro während dortiger Wahlen, Cyberattacken im Vorfeld der Krim-Annexion in 2014 oder aber gezielte Desinformationskampagnen und Cyberangriffe rund um den Bau und die Genehmigung der Pipeline Nord Stream 2: Gijsbers zeigte in einem Vortrag zum virtuellen Kongress IT meets Industry, der vom IT-Sicherheitsdienstleister Anapur veranstaltet wird, wie Russland Cyberattacken im Rahmen einer hybriden Kriegsführung nutzt. Die Auswirkungen der Attacken treffen – gewollt und ungewollt – auch die Industrie: Bereits zur letzten Präsenzveranstaltung im November 2018 hatte Gijsbers die Sicherheitsexperten der Prozessautomation mit der Aussage provoziert, dass sich diese „bereits auf einem virtuellen Schlachtfeld der Nationen befinden." „Sie werden getroffen werden und die Angreifer werden eindringen – wenn sie nicht sogar bereits eingedrungen sind."

Ob gezielter Angriff oder (gewollter) Kollateralschaden ist dabei aus Sicht der betroffenen Industrieunternehmen häufig nicht einmal klar. Jüngstes Beispiel: Der Hackerangriff auf den Satellitennetz-Provider Viasat. Das Unternehmen, das unter anderem in der Ukraine satellitengestützte Internetverbindungen anbietet, wurde exakt zum Kriegsbeginn am 24. Februar um 5 Uhr morgens Ziel eines mutmaßlich russischen Hackerangriffs: KA-Sat-Kunden waren in der Folge ohne Internet-Zugang. Doch nicht nur das ukrainische Militär war von

Autor

Armin Scheuermann ist Chefredakteur der CHEMIE TECHNIK



Im Moment sieht es nicht nach einer massiven Verschärfung aus. Aber das darf uns nicht in Sicherheit wiegen.

Dr. Felix Hanisch ist Leiter Anlagensicherheit bei Bayer und Vorstandsvorsitzender der Namur.

dem Angriff, bei dem eine Sicherheitslücke in einem Update ausgenutzt wurde, betroffen. In Deutschland waren plötzlich 3.000 Windräder, die via Satellit ferngewartet werden, nicht mehr am Netz. Über die Grenzen hinweg seien allein vom Hersteller Enercon 5.800 Windräder betroffen gewesen. Ein „Cyber-Kollateralschaden", so die Einschätzung der Bundesregierung.

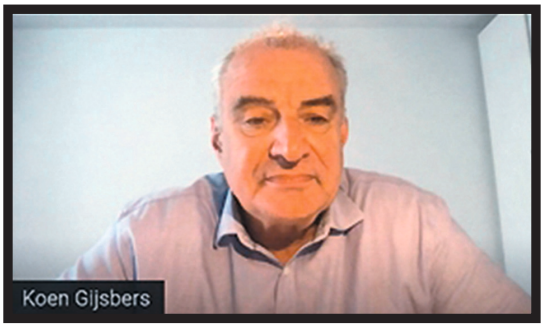
Hackerangriff provoziert politische Reaktion

Einen gezielten Angriff dagegen verübten – wiederum mutmaßlich russische Hacker – im Jahr zuvor am 29. April auf das amerikanische Pipeline-Netzwerk von Colonial Pipeline. Der Betreiber hatte aufgrund einer Ransomware-Attacke eine Pipeline abgestellt, durch die 45 % aller an der US-Ostküste verbrauchten Kraftstoffe laufen. In Teilen des Landes und insbesondere in der Hauptstadt Washington kam es daraufhin tagelang zu Engpässen in der Benzinversorgung. Am 19. Mai kündigten die USA Sanktionen gegen das russische Erdgas-Pipeline-Projekt Nord Stream 2 an. Koen Gijsbers sieht darin eine politische Reaktion der US-Regierung auf den Pipeline-Hack. Einen Zusammenhang mit dem Widerstand gegen die Genehmigung von Nord Stream 2 sieht Gijsbers auch im Ransomware-Angriff auf den Tanklogistiker Oiltanking Ende Januar 2022. In der Folge war es zu Engpässen in der Lieferkette des Tankstellenbetreibers Shell gekommen. Das Bundesamt für Sicherheit in der Informationstechnik, BSI, stufte den Vorfall als „ernst aber nicht gravierend" ein.

Diese Vorfälle untermauern die These, wonach Cyberangriffe auf die Industrie längst Teil der hybriden Kriegsführung sind und diese immer häufiger Kollateralschäden als Folge politisch motivierter Cyberangriffe zu befürchten hat. So zeigte der ehemalige Nato-General, dass die russische Not-Petya-Attake auf kritische Infrastruktur der Ukraine in 2017 Kollateralschäden in Höhe von 1,2 Mrd. US-Dollar verursacht hatte – 9 % davon entfielen auf Unternehmen aus Deutschland – darunter der Logistik-Dienstleister TNT oder der Kosmetikhersteller Beiersdorf.

Chemie im „engen Austausch" mit Behörden

In der deutschen Chemie- und Pharmaindustrie ist das Thema Cybersecurity in Folge des russischen Angriffskriegs bereits stärker in den Fokus gerückt. So berichtete Dr. Felix Hanisch, Leiter der Anlagensicherheit bei Bayer und Vorstandsvorsitzender des Anwenderverbands Namur, von einem „engen Austausch" mit Behörden und dem BSI und ließ erahnen, dass sich die Branche gegen mögliche Folgen wappnet: „Szenarien wie ein Gasembargo oder Cyberangriffe sind wichtige Aspekte, auf die wir uns vorbereiten", so Hanisch. Unter dem Schlagwort „Security for Safety" sei die Sicherheit der IT- und OT-Systeme bereits seit einigen Jahren stärker ins Bewusstsein der Branche gerückt. Gemeint ist damit die Tatsache, dass es nicht nur auf die klassische Absicherung von Gefahren aus Prozessen mit technischen Maßnahmen (funktionale Sicherheit) ankommt, sondern dass auch die Sicherheitssysteme selbst geschützt werden müssen – unter anderem vor Hackerangriffen. „Angriffe auf unsere Sicherheitssteuerungen hatten wir bei Bayer noch nicht – aber wie alle Firmen sind wir ständig Ziel zahlreicher Cyberattacken", berichtet Hanisch. Um diese abzuwehren, hat der Pharma- und Agrochemiehersteller bereits vor Jahren eine eigene Abteilung für Manufacturing IT-Security implementiert, die



Die westliche Industrie muss sich auf Gegenschläge vorbereiten. Jetzt ist es Zeit, hier in Cybersicherheit zu investieren – denn da kommt noch mehr.

Koen Gijsbers, Digital and Cyber Strategist, ehemals Leiter der Nato Communications and Information Agency.

heute Teil der IT-Organisation von Bayer ist.

Zwei Bereiche machen den Betreibern aktuell zu schaffen: Einerseits seien die verschiedenen Sicherheitsregularien unterschiedlicher Behörden zum Teil nicht widerspruchsfrei, andererseits würden Hersteller von Prozessautomatisierung teilweise die Verantwortung auf die Betreiber verlagern, wenn diese unterschiedliche Systeme zusammenschalten. „Das ist uns zu wenig. Wir können nicht hinterher Security drüber gießen, wenn keine Security drin ist."

Abgeschottete Netze

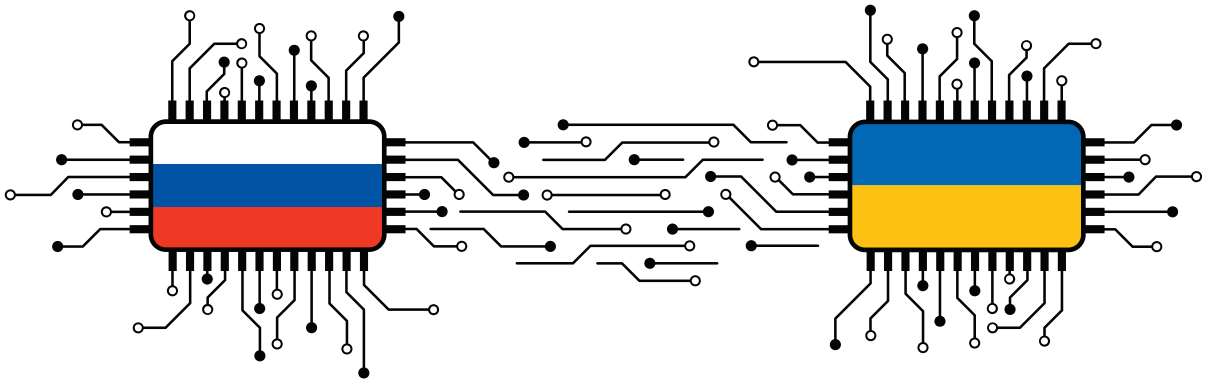
Im Hinblick auf die aktuelle Bedrohungslage infolge des Ukraine-Konflikts bleibt Hanisch vorsichtig: „Im Moment sieht es nicht nach einer massiven Verschärfung aus. Aber das darf uns nicht in Sicherheit wiegen". Koen Gijsbers warnt dagegen vor Vergeltungsangriffen durch russische Hacker als Folge der Unterstützung des Landes durch westliche Staaten: „Die westliche Industrie muss sich auf Gegenschläge vorbereiten. Jetzt ist es Zeit, hier in Cybersicherheit zu investieren – denn da kommt noch mehr." Die hybride Kriegsführung, so Gijsbers, zeichne sich dadurch aus, dass sie alle Machthebel – Desinformationen, politisch, Wirtschaft und Militär – nutze und angreife. Im Hinblick auf Sicherheitskonzepte sieht der ehemalige Leiter der Nato Communications and Information Agency eine Parallele zwischen der IT der Waffensysteme und der OT von Prozessanlagen. Hier seien abgeschottete Netzwerke, also solche, bei denen keine Verbindungen in die IT-Welt bzw. das Internet bestehen, eine wirksame Schutzmaßnahme. „Aber wir glauben, das reicht nicht aus", so Gijsbers." Wir nutzen für die nicht verbundenen Netze dieselben Standards, wie für verbundene Netze. Dadurch sind wir vorbereitet, wenn eines der Netze kompromittiert wird."

Konkret empfiehlt beispielsweise die Cyber Security Allianz Five Eyes, in der sich Großbritannien, Australien, Kanada, Neuseeland und die USA zusammengeschlossen haben, aktuell Unternehmen, sich verstärkt um Updates in Betriebssystemen, Anwendungssoftware und Firmware zu kümmern und in IT-Netzwerken ein zentrales Patch-Management zu implementieren. Für Betriebs- bzw. OT-Netze sollte eine Risikobetrachtung für das Patch-Management durchgeführt werden. Außerdem sollten starke Passwörter und Mehrfaktor-Authentifizierung für den Zugang zu Systemen implementiert werden. Und schließlich komme es auf die Wachsamkeit der Endanwender an. Diese zu trainieren, hält auch Felix Hanisch für eine der wichtigsten Maßnahmen im Hinblick auf OT-Security.

Weil sich die Angriffe verändern, sei es zudem wichtig, die Cybersecurity-Maßnahmen ständig zu erneuern. Gijsbers, der 1980 als Sprinter und Mittelstreckenläufer bei den olympischen Spielen mit dabei war, empfiehlt Wettbewerbe und Übungen zum Thema zu veranstalten. „Niemand möchte Verlierer sein – deshalb steigt durch solche Maßnahmen sukzessive das Qualitätsniveau." ●

Entscheider-Facts

- *Ob gezielter Angriff oder „nur" Kollateralschaden: Die Industrie ist immer stärker von Cyberattacken betroffen.*
- *Weil der Westen die Ukraine unterstützt, ist vermehrt mit russischen Hackerangriffen zu rechnen.*
- *Unternehmen sollten verstärkt Maßnahmen gegen die Bedrohungen treffen.*



Der Russland-Ukraine-Konflikt wird nicht nur mit physischen Waffen, sondern auch mit massiven Cyberattacken geführt.

Bild: Mark Rademaker – AdobeStock