Cybersecurity in Produktionsprozessen

Cyberangriffe auf Unternehmen mit Produktionsanlagen verursachen Millionenverluste. Von der Vorstellung, alle Einfallstore für Angreifer durch Abwehrmechanismen schließen zu können, sollten sich Sicherheitsverantwortliche jedoch verabschieden. Die Herausforderung liegt in der Prävention von Angriffen und der schnellen Erkennung von IT-Sicherheitsproblemen und Cyberangriffen.

VON MARTIN SCHRAMM

LAUT EINER UMFRAGE des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV) schätzen 72 Prozent der Unternehmen das Risiko eines Cyberangriffs als hoch oder sehr hoch ein, allerdings halten nur 34 Prozent einen Angriff auf das eigene Unternehmen für wahrscheinlich. Viele Firmen vertreten den Irrglauben, dass sie zu klein oder die gespeicherten Daten zu unwichtig seien, um in den Fokus von Cyberkriminellen zu geraten. Cyberangriffe erfolgen meist nicht gezielt und treffen alle Unternehmen, die in irgendeiner Form am Netz hängen, unabhängig von deren Mitarbeiterzahl oder Brisanz der Daten.

Die Motive der Hacker sind vielfältig: Staatsgetriebene Aktivitäten zielen darauf ab, betrügerisch an Informationen zu kommen, oder Services und Infrastruktur lahmzulegen. Unternehmen sind beispielsweise an Industriespionage interessiert oder daran, Konkurrenten auszuschalten. Kriminelle Individuen oder Netzwerke wiederum nutzen oftmals persönliche Informationen zur Erpressung von Geldzahlungen.

Störungen wirken sich auf Produktionsbetrieb aus

Cybersecurity spielt in jedem vernetzten Unternehmen eine große Rolle. Jede Beeinträchtigung im Produktionsbetrieb wirkt sich unmittelbar auf den Fertigungsprozess des Unternehmens und somit auch auf die Distribution aus. Kommt es zu Verzögerungen in der Lieferkette, kann dies zu Vertragsstrafen oder auch Klagen und Rufschädigung führen. Das Risiko eines Cyberangriffs wird hier mittlerweile als genauso schädigend eingestuft wie die Unterbrechung des Betriebs durch Naturgewalten. Die eigenen Systeme abzusichern, liegt im Einflussbereich des Unternehmens, innerhalb der Lieferkette ist dies jedoch nur bedingt möglich. Deshalb ist es für die Produktion besonders wichtig, mögliche Risiken zu kennen und sich gegen Angriffe bestmöglich vorzubereiten.

Dabei sind drei verschiedene Risikobereiche zu beachten:

1. Risiken, die den ordentlichen Geschäftsbetrieb des Unternehmens beeinflussen, beispielsweise die Produktion, den Vertrieb oder die Rechnungslegung
2. Risiken, die rechtliche und vertragliche Konsequenzen für das Unternehmen nach sich ziehen können
3. Risiko der Rufschädigung

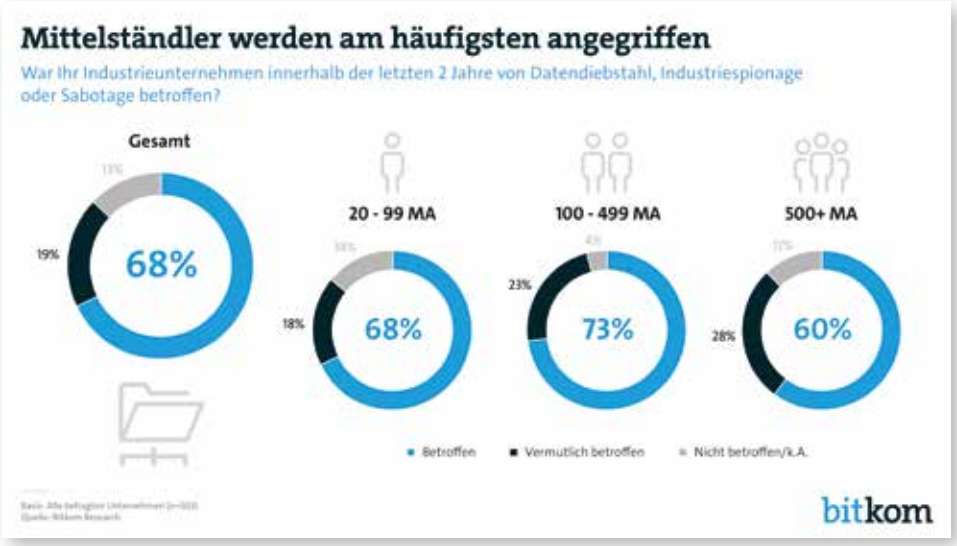
Betriebsrisiken wie auch die finanziellen Folgen rechtlicher Dispute lassen sich heute umfassend versichern. Die Folgen, die eine Rufschädigung und ein damit verbundener Vertrauensverlust von Kunden mit sich bringen, sind nur schwer steuerbar.

Informationssicherheit als Teil der Unternehmenskultur

Cybersecurity sollte in allen Prozessen des Unternehmens implementiert werden, sodass jede externe Transaktion, ob sichtbar oder im Hintergrund, geschützt ist. Sicherheit ist somit ein unternehmensweites Thema, das Veränderungen mit sich bringt und auf der Führungsebene beginnt. Es ist Aufgabe des Managements, Sicherheit als Teil der Betriebskultur zu kommunizieren.

Unterhalb der Chefetage trägt der CISO (Chief Information Security Officer) die Verantwortung für die Informationssicherheit im Unternehmen. Das Risikomanagement sollte daher auf Cybersicherheit ausgerichtet sein. So ermöglicht zum Beispiel die Einführung eines Informationssicherheits-Managementsystems (ISMS) nach dem Regelwerk ISO 27001, die Informationssicherheit im Unternehmen dauerhaft zu steuern und zu verbessern.

Der CISO oder wahlreise auch ein externer Sicherheitsexperte analysieren



68 Prozent der Unternehmen wurden in den Jahren 2017 bis 2018 angegriffen. Quelle: Bitkom Research

die Prozesse, Programme und Hardwareausstattung auf Schwachstellen. Im nächsten Schritt überprüft er, welche Hard- und Softwarelösungen eingesetzt werden sollten. Externe Lösungen, zum Beispiel ausgelagerte Security Operation Center (SOC), gewinnen zunehmend an Bedeutung. Sie sind oft sicherer als Inhouse-Lösungen, allerdings sollte der Provider einem Due-Diligence-Prozess unterzogen werden.

Mitarbeiter als wichtige Schnittstelle zum CISO

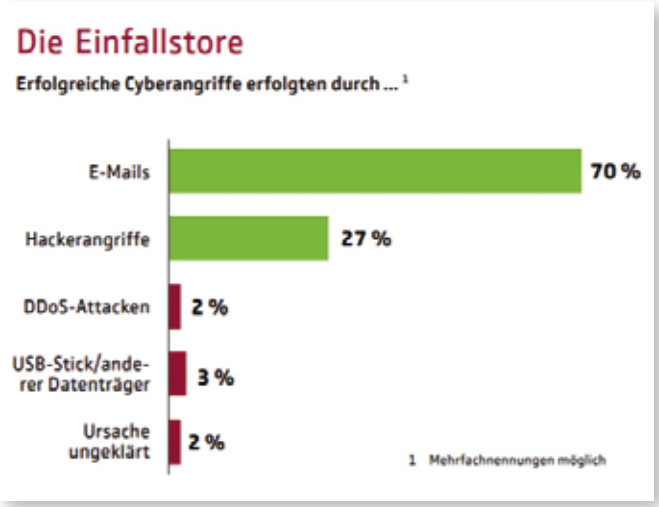
In jedem Team sollte eine Person direkten Zugang zum CISO erhalten. Denn es gilt vor allem, die Mitarbeiter mit ein zu beziehen, da sie Opfer von Angriffen sein können. So stellen laut einer Studie des GDV E-Mails mit 70 Prozent nach wie vor das größte Einfallstor für Hacker dar. Deshalb empfiehlt es sich, Regeln für den Umgang mit E-Mails aufzustellen und die Mitarbeiter kontinuierlich zu schulen, beispielsweise mit Übungen, bei denen verschiedene Szenarien durchgespielt und Abläufe für den Krisenfall festgelegt werden.

Nicht alle Daten sind gleich wichtig. Ein Inventar hilft, diese nach Wichtigkeit zu klassifizieren. Die wertvollsten Daten genießen den höchsten Schutz. Um die Daten zu sichern, sollten regelmäßig Backups durchgeführt und diese auf Funktionalität, Konsistenz und Aktualität getestet werden. Außerdem sinkt das Risiko eines Cyberangriffs, wenn die eingesetzte Soft- und Hardware stets auf dem neusten Stand gehalten und Sicherheits-Updates sofort installiert werden.

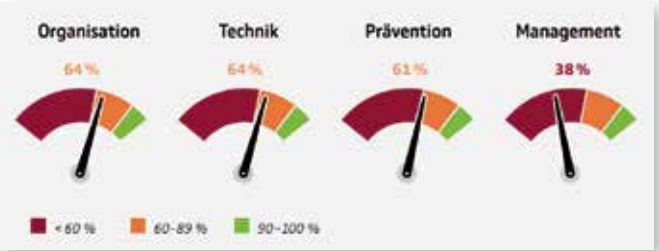
Isolierter Betrieb der Systeme im Produktionsprozess

Infrastruktursysteme, die direkt mit dem Produktionsprozess zusammenhängen oder diesen steuern, sollten isoliert von vernetzen Systemen laufen. Wenn diese mit externen Systemen kommunizieren, ist das allerdings nur bedingt möglich. Integrierte Lieferketten sind offen, um den Kunden schnellstmöglich beliefern zu können. Zum Beispiel kann der Kunde bei der Bestellung eines neuen Fahrzeugs dessen Spezifikationen online konfigurieren, die dann unmittelbar zur nächst verfügbaren Produktionsstätte der Herstellers übermittelt werden. Das erfordert einen besonderen Schutz der Kommunikationswege vor Manipulation durch Hacker. Demnächst könnten hier Smart Contracts einen wirksamen Schutz bieten.

Der US-amerikanische Nahrungsmittelkonzern Mondelez, der unter anderem die Marken Toblerone und Oreo führt, wurde Opfer eines Cyberangriffs durch die Malware „Petya". Dadurch wurde der Zugang zu 1.700 Servern und 24.000 Notebooks gekappt. Mitarbeiter konnten keine E-Mails mehr versenden und nutzten daher WhatsApp für die Kommunikation. Es entstand ein Schaden in Höhe von über 100 Millionen US-Dollar. Im darauffolgenden Quartal verzeichnete Mondelez einen Umsatzrückgang von fünf Prozent, wovon die Hälfte dem Angriff geschuldet war. Angriffe mit der Petya-Malware, ausgeführt in der Ukraine von russischen Hackern, erfolgten auch auf die Konzerne Merck, Maersk und FedEx, die aber über ein funktionierendes Sicherheitssystem verfügen. Für Mittelständler und Familienunternehmen ist es allerdings schwierig, ihre Prozesse und Systeme entsprechend abzusichern.



E-Mails sind das wichtigste Einfallstor bei Mittelständlern.
Quelle: Ergebnisse der Forsa-Befragung „Cyberrisiken im Mittelstand".



In der Organisation und Technik halten sich deutsche Unternehmen für gut aufgestellt. Quelle: GDV Lagebericht Cyberrisiken 2019.

Szenario: Ein Hackerangriff liegt vor

Kommt es zu einem Angriff, ist es sinnvoll einen Notfallplan in der Tasche zu haben. Denn bei einer Cyberattacke können wenige Minuten entscheiden, ob Unternehmen die Kriminellen noch fassen können und wie groß der Schaden letztlich wird. Es muss daher definiert werden, welche Maßnahmen in welcher Reihenfolge bei einer Cyberattacke zu durchlaufen sind und wer wann zu informieren ist. Die Datenschutzgrundverordnung verlangt von Unternehmen, ihre Daten innerhalb von 72 Stunden sicherzustellen. Der Schaden für das einzelne Unternehmen wird bestimmt durch folgende Priorisierung:

- Was sind die wichtigsten IP-Werte des Unternehmens und wie wurden sie gesichert?
- Wo sind diese Werte/Daten gespeichert und wie geschützt?
- Wie werden Dritte wie Zulieferer und Dienstleister auf ihre Cybersicherheit untersucht?
- Werden Standards wie NIST oder ISO27001 eingehalten?
- Szenario durchspielen: Was kann schiefgehen und welchen Einfluss hätte dies?
- Ist im Notfallplan eine Kommunikationsstrategie integriert?
- Was würden die aktuellen Versicherungspolicen abdecken, bei welchen Szenarien?

Dass kriminelle Attacken deutsche Industrieunternehmen besonders hart treffen, zeigt eine Bitkom-Studie: Durch Sabotage, Datendiebstahl oder Spionage ist in den Jahren 2017 und 2018 ein Schaden von insgesamt 43 Milliarden Euro entstanden. Hierbei sind in den beiden Jahren sieben von zehn Unternehmen Opfer solcher Angriffe geworden. Höchste Zeit also, in IT-Sicherheit zu investieren und Strategien für die Daten- und Systemsicherheit auszuarbeiten. sg

Martin Schramm ist freiberuflicher Berater, spezialisiert auf Strategieberatung in Cybersecurity und Versicherungslösungen. Er gehört dem Experten-Netzwerk von Comatch an.