Cybersicherheit in der Produktion – die 8 wichtigsten Aspekte

CYBERANGRIFF AUF CYBERANGRIFF – DAS „GESCHÄFT" VON CYBERKRIMINELLEN FLORIERT. Hatten sie bislang vorrangig die klassische IT im Visier, rückt nun auch die Operational Technology, kurz OT, in den Fokus. Die Systeme in Fertigung und Produktion sind ja auch lohnende Ziele. Erfahren Sie hier acht wichtige Informationen zur Cybersicherheit in Ihrer Produktion.

1. Cyberkriminelle attackieren Produktionssysteme

Wenn es in der Öffentlichkeit um Cyberkriminalität geht, dann denkt man meist an den klassischen Datenklau – Kundendaten werden über einen Cyberangriff auf die IT von Unternehmen oder über die bekannten Phishing-Mails erbeutet und dann missbraucht.

Tatsächlich ist aber auch das produzierende Gewerbe, so der Gesamtverband der Deutschen Versicherungswirtschaft (GDV), ein beliebtes Ziel von Cyberkriminellen.

Unter Berufung auf eine Forsa-Studie schreibt der Verband, dass 26 Prozent der befragten Unternehmen aus der Elektro-, Chemie- und Lebensmittelindustrie sowie dem Maschinenbau und der kunststoffverarbeitenden Industrie bereits durch Cyberangriffe geschädigt wurden. Satte 71 Prozent gaben an, dass ihr Betrieb durch einen mehrtägigen Ausfall der IT eher stark bis sehr stark eingeschränkt würde.[1]
Wichtig für das Verständnis: Neben dem direkten Schaden und dem Imageverlust können auch Schadensersatzforderungen von Kunden sowie rechtliche Konsequenzen drohen.

2. „Geschäftsmodelle" der Cyberkriminalität

Laut des Bundeskriminalamts ist „Cybercrime eines der sich am dynamischsten verändernden Kriminalitätsphänomene. Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt".[2]

Der breiten Öffentlichkeit bekannt sind vorrangig die großen Fälle von Datendiebstahl – Hacker dringen in die IT-Systeme von Unternehmen ein, um Kundendaten zu stehlen. Diese werden dann in der Regel im Darknet vermarktet und für weitere kriminelle Handlungen eingesetzt.

Über Phishing-Mails ergaunerte Kreditkarten- oder, schlimmer noch, Zugriffsdaten auf andere Systeme, werden direkt für Finanztransaktionen oder eben den Einbruch in Unternehmensnetze verwendet.
Ein weiteres, und leider ebenso florierendes, Modell ist die Erpressung von Unternehmen. Cyberkriminelle dringen in die Systeme ein, blockieren diese und geben sie erst nach Zahlung eines Lösegeldes, meist in Bitcoin, wieder frei. Das Magazin IT&Production schreibt unter Berufung auf eine Studie des Branchenverbandes Bitkom, dass sich die Zahl solcher Fälle seit 2019 bis heute nahezu vervierfacht hat.[3] Dieses Modell ist für produzierende Unternehmen eine große Gefahr.

3. Wachsende Risiken durch IoT und Homeoffice

Bislang waren IT-Systeme beispielsweise in Management, Marketing und Vertrieb mehr oder minder getrennt von denen der OT, der Operational Technology in der Produktion. Durch die fortschreitende Konvergenz von IT und OT, Stichworte sind IoT und Industry 4.0, wachsen die Systeme immer enger zusammen – und damit verschärft sich die Gefahrenlage.

Auch durch den pandemiebedingten Boom in Sachen Homeoffice nimmt die Angriffsfläche weiter zu. Meist sind die Heimnetzwerke im privaten Bereich deutlich unzureichender geschützt als die Systeme im Unternehmen und das Bewusstsein für IT-Sicherheit ist zuhause erfahrungsgemäß weniger ausgeprägt – damit ist das Homeoffice ein Risikofaktor.

4. „Professionalisierung" der Cyberkriminalität

Cyberangriffe sind ein sehr attraktives „Business" geworden, daher werden auch die Cyberangriffe immer professioneller. Ein Zeichen dafür sind die immer perfekteren Phishing-Mails, die auch für darin geübte Personen oft kaum mehr erkennbar sind. Ein weiteres Beispiel sind E-Mails, die wie interne Nachrichten etwa der CEOs wirken und zu bestimmten Aktionen, wie etwa die Ausführung von Überweisungen, auffordern (CEO-Fraud). Auch die Geschwindigkeit solcher Angriffe ist beeindruckend – oft reichen wenige Schritte aus, um in ein fremdes System einzudringen.

1) https://www.gdv.de/resource/blob/67186/b85a48cd0808c19fb6681158fa563114/cyberreport-ausgabe-als-pdf-data.pdf
2) https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html
3) https://www.it-production.com/news/hoher-schaden-fuer-die-deutsche-wirtschaft/

5. Mythen und Fehleinschätzungen

Laut dem GDV schätzen zwar 56 Prozent der in der Studie befragten produzierenden Unternehmen das Risiko für Cyberkriminalität für ihre Branche als hoch bis sehr hoch ein – aber nur 42 Prozent für ihr eigenes Unternehmen.

Laut der Studie sagen ...

- 62 Prozent, dass ihr Unternehmen zu klein sei, um in den Fokus von Cyberkriminellen zu geraten
- 55 Prozent, dass ihre Daten für Cyberkriminelle nicht interessant seien
- 77 Prozent, dass ihre IT-Systeme umfassend geschützt seien
- 54 Prozent, noch nie Opfer von Cyberangriffen gewesen zu sein.

Diese „Irrglauben und Beruhigungspillen" zeigen, so der GDV, dass das Bewusstsein für die Gefahren durch Cyberkriminalität in der Produktion noch kaum ausgeprägt ist.

6. Cybergefahren im Überblick

Cyberkriminelle ziehen alle Register, wenn es darum geht, Zugriff auf die Systeme ihrer Opfer zu erhalten, um sie auf die eine oder andere Weise zu schädigen. Hier eine kurze Übersicht – ohne Anspruch auf Vollständigkeit:

Einschleusen von Malware: Schon fast der Klassiker im Bereich Cybersicherheit ist die Malware – Schadprogramme, die über das Internet eingeschleust werden – dazu genügt der Klick auf einen Link in einer gefälschten Mail. Die „Infektion" ist auch über USB-Sticks möglich. Über solche Schadsoftware können Hacker die Kontrolle über (Produktions-) Systeme erhalten oder sie nutzen den Zugang zur Industriespionage. Eine Untermenge von Malware ist die Ransomware – sie blockiert Systeme ganz oder teilweise, die dann erst nach Zahlung eines Lösegeldes wieder freigeschaltet werden.

Kompromittierung von Extranet- und Cloud-Komponenten: Viele Unternehmen nutzen heute cloudbasierte Dienstleistungen externer Servicepartner – Stichworte sind beispielsweise SaaS, IaaS und Onlineshop-Lösungen. Wenn die Systeme der externen Dienstleister nicht optimal abgesichert sind – das gilt auch für die sichere Trennung der verschiedenen Mandanten – stellen sie ein Sicherheitsrisiko dar.

Per Internet verbundene Steuerungskomponenten: In diesem Bereich hat der „Computerwurm" Stuxnet schon im Jahre 2010 traurige Berühmtheit erlangt – er fokussiert sich auf industrielle Systeme zur Überwachung und Steuerung technischer Prozesse in einer automatisierten Fertigung (SCADA). Fatal: Es existiert sogar eine Suchmaschine, mit der Systeme mit offenen TCP/IP-Ports gefunden werden können. Sie kann für Sicherheitsanalysen genutzt werden, findet aber auch Zuspruch bei Hackern.

Einbruch über Fernwartungszugänge: Oft werden Maschinen durch eigene Techniker oder Experten der Hersteller aus der Ferne gewartet. Die entsprechenden Schnittstellen können unzureichend geschützt sein. So können Hacker Zugang erlangen und etwa die Steuerung der Maschinen übernehmen.

Kompromittierung von Smartphones im Produktionsumfeld: Immer wieder fordern die Hersteller von Smartphones, oder allgemein mobiler Endgeräte, die Nutzer auf, Sicherheitsupdates zu installieren. Allein das ist schon ein Indiz, welche Gefahren von den auch im Unternehmen genutzten Privatgeräten ausgehen. Nicht ohne Grund gelten Smartphones auch als „smarter Touchpoint" für Cyberkriminelle.

DDoS-Angriff: Hierbei werden die Systeme der betroffenen Unternehmen über Anfragen oder Datenübertragungen in enorm hoher Zahl bis hin zum Funktionsausfall überlastet. „Sinn und Zweck" dieser Angriffe ist die bloße Schädigung oder auch die Erpressung der Unternehmen.

Menschliches Fehlverhalten: Wohl die häufigsten Ursachen und damit die größten Bedrohungen sind menschliches Fehlverhalten oder Sabotage. Dies kann der unbedarfte Klick auf den Link in einer gefälschten E-Mail oder auch das bewusste Einschleusen von Schadsoftware etwa durch enttäuschte oder gekündigte Mitarbeitende sein.

7. Maßnahmen zum Schutz vor Cyberkriminalität

Wenn Unternehmen wissen, wie sie Angriffswege unterbrechen können, können sie die Gefahren durch Cyberangriffe deutlich verringern – folgend geben wir einen Überblick über mögliche Maßnahmen zum Schutz.

Softwarequalität und -aktualität: Achten Sie darauf, dass nur Softwarelösungen seriöser Hersteller eingesetzt werden. Sorgen Sie außerdem dafür, dass diese immer aktuell gehalten werden, verpassen Sie kein Sicherheitsupdate.

Zugriffsrechte managen: Eine oft unterschätzte Aufgabe ist das Management der Zugriffsrechte. Das bezieht sich unbedingt auch auf Mitarbeitende, die aus dem Unternehmen ausscheiden – diesen müssen sofort alle Zugriffsrechte aberkannt werden.

Sicherheitsmaßnahmen „gemäß Stand der Technik": Implementieren Sie möglichst eine Sicherheitslösung, die anerkanntermaßen auf dem neuesten Stand der Technik ist und vom jeweiligen Hersteller fortlaufend über Sicherheitsupdates gepflegt wird.

Bewusstsein schaffen: Ein wichtiger Aspekt ist das Bewusstsein der Mitarbeitenden für Fragen der IT-Sicherheit. Einerseits bezieht sich dies auf die nötige Sensibilität im Umgang etwa mit Phishing-Mails, andererseits auch auf die Fähigkeit, Indizien einer möglichen Kompromittierung zu erkennen. Letzteres ist wichtig, da im Falle eines Cyberangriffs sehr schnell reagiert werden sollte, um den Schaden in Grenzen halten zu können.

IT-Security-Audit durchführen: Unterziehen Sie Ihre Systeme – all Ihre Systeme, auch die in der Produktion – einem Sicherheitsaudit. So ermitteln Sie etwaige Schwachstellen, die für Cyberangriffe ausgenutzt werden könnten. Arbeiten Sie dazu am besten mit einem externen Dienstleister zusammen, der die Systeme im Rahmen eines „Cold Eye Reviews" unvoreingenommen analysiert.

Entwicklung und Umsetzung eines Maßnahmenplans: Entwickeln Sie auf Basis der Ergebnisse des Audits einen schriftlichen Maßnahmenplan für den Fall eines Cyberangriffs, der auch Ihre externen Dienstleister einbezieht.

8. SAP-Security im Produktionsumfeld

Applikationen von SAP werden unternehmensweit eingesetzt, nicht nur in Verwaltung, Marketing und Vertrieb, sondern auch in der Produktion. Beispiele sind SAP PP für die Produktionsplanung und -steuerung oder auch SAP Manufacturing Execution für die Steuerung, Überwachung und Automatisierung von Fertigungsprozessen.

Fachleute sprechen von einem „SAP-Security-Dilemma". Einerseits bilden die SAP-Applikationen eben meist das Rückgrat der Softwareumgebung – andererseits ist ihre Anbindung an die bekannten Security-Systeme schwierig. Dabei ist der Schutzbedarf unabhängig vom gewählten Betriebsmodell für die Nutzung der Applikationen (Azure, AWS, Google Cloud, On Premises).

Eine bekannte Sicherheitslösung ist Microsoft Sentinel. Dabei handelt es sich um eine cloudnative Lösung für das Security Information und Event Management (SIEM) und die Sicherheitsorchestrierung, Automation und Reaktion (SOAR). Microsoft Sentinel bietet intelligente, unternehmensweite Sicherheits- und Bedrohungsanalysen samt der Erkennung von Bedrohungen und Angriffen sowie den entsprechenden Reaktionen darauf.

Für diese Lösung steht nun ein von Microsoft und SAP unter Beteiligung von Arvato Systems entwickelter Connector für SAP-Systeme zur Verfügung. Dieser erfasst verschiedenste SAP Logs und übergibt diese an Microsoft Sentinel für die genannten Sicherheitsanalysen. Somit kann das SAP-System fortlaufend – auch nach Dienstschluss – automatisiert auf verdächtiges Verhalten hin überwacht werden.

So kann auf effiziente Weise auch den Sicherheitsvorgaben entsprochen werden, die das Bundesamt für Sicherheit in der Informationstechnik in Bezug auf SAP-Systeme herausgegeben hat.[4]

4) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/06_APP_Anwendungen/APP_4_2_SAP_ERP_System_Edition_2021.pdf?__blob=publicationFile&v=2

Ihre Kontakte für SAP Security in der Fertigungsindustrie

Achim Reupert

Experte für IT-Security in der Fertigungsindustrie

Tel: +49 5241 80-49541

Daniel Heer

Experte für IT-Security in der Fertigungsindustrie

Tel: +49 5241 80-88577

ÜBER ARVATO SYSTEMS

Arvato Systems unterstützt als international agierender IT-Spezialist namhafte Unternehmen bei der Digitalen Transformation. Ausgeprägtes Branchen-Know-how, hohes technisches Verständnis und ein klarer Fokus auf Kundenbedürfnisse zeichnen uns aus. Im Team entwickeln wir innovative IT-Lösungen, bringen unsere Kunden in die Cloud, integrieren digitale Prozesse und übernehmen den Betrieb sowie die Betreuung von IT-Systemen.

Wir bieten:

- Umfassende IT-Lösungen für Branchen wie Handel, Medien, Fertigungsindustrie, Gesundheitswesen, öffentlicher Sektor sowie Energie- und Versorgungswirtschaft
- Langjährige Erfahrung in der Digitalen Transformation
- Kompetenz in Themen wie Künstliche Intelligenz, Cloud Computing, IT-Security, Customer Experience, E-Commerce und Business Process Management
- Know-how in vielen starken Technologien und ein ausgeprägtes Ökosystem mit Partnern wie Amazon Web Services, Google, Microsoft und SAP
- Eine große Bandbreite an Infrastructure Services wie beispielsweise Managed Services sowie ein darauf aufbauendes Application Management

Als Teil von Bertelsmann stehen wir auf dem soliden Fundament eines deutschen Weltkonzerns. Zugleich setzen wir auf unser starkes strategisches Partner-Netzwerk mit internationalen Top-Playern wie AWS, Google, Microsoft oder SAP. Wir machen die digitale Welt einfacher, effizienter und sicherer und unsere Kunden erfolgreicher.

We Empower Digital Leaders.

ARVATO SYSTEMS