CHUBB®

Risk Newsletter
2/2019

Alle digitalen Risiken im Blick

Um über die Versicherbarkeit von Cyberrisiken zu entscheiden, stehen klassischerweise Fragen zur IT-Sicherheit und zum Datenschutz im Fokus der Bewertung. Ein rein auf die IT beschränkter Blick ist hierbei aber längst nicht ausreichend, um das vollumfängliche Cyberrisiko eines Unternehmens analysieren und beurteilen zu können. Vielmehr gilt es beim Cyber-Underwriting das große Ganze zu erfassen, weshalb neben der Sicherheit der Verwaltungsumgebung auch die Sicherheit der Produktionsumgebung eines Unternehmens einen ebenso unerlässlichen Faktor darstellt. Besonders wichtig ist das Thema nicht zuletzt vor dem Hintergrund, dass jene „Operational Technology“ (OT) bzw. operative Technologie seit Jahren zunehmend externen Risiken ausgesetzt ist. Die Ursache hierfür liegt in der immer weiter voranschreitenden Digitalisierung, durch welche OT und klassische IT stetig mehr miteinander verschmelzen. Ein Beispiel dafür ist die zunehmende Automatisierung innerhalb von Produktionsanlagen und kritischen Infrastrukturen, d.h. die Überwachung der OT von Bohranlagen und Verteilnetzen für Öl und Gas, Energieerzeugungs- und Verteilsystemen, der Herstellung von chemischen und pharmazeutischen Produkten und Konsumgütern und neben vielem anderen auch in Einrichtungen des Gesundheitswesens, des Transportwesens und der Telekommunikation. Wirtschaftlich hat dies enorme Vorteile, doch genau diese Entwicklung führt auch dazu, dass operative Technologie heute verstärkt von Cyberrisiken beziehungsweise -angriffen betroffen sein kann.

Großes Schadenpotenzial

All jene Unternehmen, die rein auf Basis ihrer Geschäftstätigkeit eine hohe Risikoexponierung für Betriebsunterbrechungen bedingt durch den Ausfall von Systemen innerhalb ihrer OT aufweisen, suchen im aktuellen Marktumfeld nach einem entsprechenden Versicherungsschutz. Eine hinreichende Absicherung ihrer Risiken ist häufig allerdings nicht vollends gegeben. Zwar zeigt die bisherige Schadenerfahrung, dass klassische Angriffsvektoren, wie die Infizierung mit Malware, Phishing, Brute Force-Attacken auf Passwörter, bei denen wahllos verschiedene Buchstabenfolgen oder Zeichenketten automatisiert ausprobiert werden, oder Ransomware, primär die Verwaltungsumgebung eines Unternehmens attackieren. Dennoch sind zahlreiche Beispiele aus der Praxis vorhanden, die belegen, dass Angriffe auf OT-Systeme insgesamt zunehmen. Diese können zum Beispiel zu Angriffen auf Hochöfen in Stahlfabriken, zur Abschaltung von Sicherheitsüberwachungssystemen in Kernkraftwerken oder zur Manipulation der Wärmesteuerung großer Medikamentenlager führen - alles Szenarien mit enormem Schadenpotenzial. ▶

Prioritäten kennen

In Bezug auf eine professionelle Absicherung der operativen Technologie stellt sich aus Underwriting-Sicht daher grundsätzlich die Frage, was die generellen „Eckpfeiler“ sind, die es in besonderem Maße in Sachen Versicherbarkeit zu berücksichtigen gilt. Es macht Sinn, bei dieser Betrachtung primär die drei vordergründigen Schutzziele der Informationssicherheit in den Fokus zu stellen – Vertraulichkeit, Integrität und Verfügbarkeit. Diesen Schutzzielen widmet sich im Allgemeinen auch die OT-Sicherheit, allerdings mit einer etwas anderen Gewichtung als innerhalb der klassischen IT. Im Bereich der operativen Technologie ist die Verfügbarkeit ein primäres Schutzziel, da die Verfügbarkeit der Produktionssysteme bei herstellenden Unternehmen den Kern der Wertschöpfung darstellt.

Mehr Sicherheit – aber wie?

Bei der Sicherheit der operativen Technologie wird prinzipiell mit den gleichen „Waffen gekämpft“ wie innerhalb der IT-Sicherheit. Was hier allerdings erschwerend hinzukommt: Systeme innerhalb der OT haben eine wesentlich längere Lebensdauer als jene der IT, zudem sind ein Patching – im Allgemeinen und in Abhängigkeit von den Maschinen – und Antiviren-Software für diese entweder nicht möglich oder nur sehr schwer umzusetzen. Konkrete Gegenmaßnahmen zum Schutz der OT-Systeme bestehen daher vor allem in einer umfassenden Segmentierung des Netzwerks durch eine Trennung der IT von der OT, die zusätzlich durch Firewalls abgesichert ist. Weitere Schritte sind ein allgemeines Netzwerk-Monitoring als auch eine kontinuierliche Konfigurationskontrolle der Applikationen und Nutzerzugriffe. Sogenanntes „Whitelisting“, mit dessen Hilfe lediglich freigegebene, vertrauenswürdige Software ausgeführt wird, kann dazu beitragen, das Einschleusen von Malware in das Produktions-LAN über offene USB-Zugänge zu verhindern. Zusätzlich gilt es auch durch technische Möglichkeiten sicherzustellen, dass sich fremde Geräte erst gar keinen Zugriff zum Produktions-LAN verschaffen können.

Einfallstore schließen

Ein umfassender Überblick und eine ganzheitliche Dokumentation über den allgemeinen Aufbau der vollständigen Netzwerkumgebung sind fundamental. Auch wenn Malware häufig zunächst das Büronetzwerk infiltriert und sich anschließend erst über eine horizontale und vertikale Rechteausweitung weiter bis in die Produktionsumgebung ausweiten kann, ist es prinzipiell möglich, dass weitere Einfallstore vorhanden sind, die eine Kompromittierung der Produktionsumgebung ermöglichen. Möglich ist ein Zugang beispielsweise auch über ungesicherte Modems, nicht hinreichend geprüfte und unsichere Zugriffe externer Dienstleister, offene WLAN-Schnittstellen, fehlkonfigurierte Firewalls oder infizierte Geräte, die sich aufgrund einer fehlenden Identifikation und Authentisierung direkt mit dem Netzwerk verbinden können. Ein noch umfassenderer Schutz kann in der Regel nur gegeben werden, wenn nicht nur eine logische Segmentierung zwischen der IT und der OT vorliegt, sondern eine vollkommen physische (sogenanntes „Air-Gapping“). Im Falle eines lokalen Ausfalls wäre die Verfügbarkeit des restlichen Netzes somit nämlich ungefährdet. Möglich sind in diesem Zusammenhang aber auch unidirektionale, also nur in eine Richtung fungierende Schnittstellen aus dem Produktionsnetzwerk in das herkömmliche Unternehmensnetz. Hierbei ist allerdings zu beachten, dass in Produktionsbetrieben häufig über ein zentrales System Arbeitsaufträge direkt an die Maschinen gesendet werden und diese eventuell auch Rückmeldungen geben müssen.

Viel zu tun

Damit Sicherheitsmaßnahmen auch tatsächlich greifen können, ist es entscheidend, diese im Unternehmen zu etablieren und nicht zuletzt auch auf höchster Ebene zu verankern. Im Idealfall sind daher Risikobewertungen im Hinblick auf die OT in das Risikomanagement eingebunden. Häufig ist dies zwar schon der Fall, jedoch beziehen sich jene Bewertungen in der Praxis zumeist eher auf die Verfügbarkeit von Strom, Material und Sicherheit als auf die Einflüsse durch Cyberangriffe. Werden Sicherheitsrichtlinien und -standards definiert, ist es wiederum wichtig, diese so gut wie möglich auf die jeweiligen besonderen Erfordernisse der operativen Technologie abzustimmen und nicht zuletzt auch deren Umsetzung in der Praxis regelmäßig zu prüfen. Mit Hilfe von Schulungen speziell zur OT-Sicherheit können zudem Mitarbeiterinnen und Mitarbeiter in der Produktion dabei unterstützt werden, jene Sicherheitsstandards ▶

einzuhalten. Spezifische OT-Reaktionspläne tragen außerdem dazu bei, entsprechende Verantwortlichkeiten zu belegen und zu dokumentieren. Vor diesem Hintergrund erweist es sich auch als sinnvoll, neben dem allgemeinen IT-Sicherheitsbudget ebenfalls ein gesondertes, zusätzliches Budget für die OT-Sicherheit zur Verfügung zu stellen. Hierbei ist es aufgrund der teilweise unterschiedlichen Ausrichtung von OT und IT außerdem von Vorteil, wenn jene Budgets von Personen verwaltet werden, die die konkreten unternehmensinternen Sicherheitsanforderungen an die operative Technologie im Detail kennen und verstehen. Nichtsdestotrotz ist ein kontinuierlicher Austausch zwischen den beiden Bereichen unentbehrlich, denn auch für die operative Technologie gilt schließlich: Die Digitalisierung ist in vollem Gange!

Benedikt Klingenheben
Underwriter Cyber
benedikt.klingenheben@chubb.com

Über den Autor

Benedikt Klingenheben ist seit September 2018 Underwriter Cyber bei Chubb in Düsseldorf und im neuen Segment Middle Market zuständig für die Regionen Nord und West. Der Kaufmann für Versicherungen und Finanzen sowie Master-Absolvent in Versicherungswesen von der Technischen Hochschule Köln ist zusätzlich als „Certified Information Systems Security Professional“ (CISSP) zertifiziert.

Chubb. Insured.[SM]