Bedarfsorientierte Cybersicherheit für KMU

In guten Händen

von Nico Werner

Die Komplexität und Vielfalt der Technologien für Geschäftsprozesse nehmen rasant zu. Gleichzeitig steigen potenzielle Risiken und Gefahren. Kommt es zu Hackerangriffen oder Ausfällen durch technisches oder menschliches Versagen, kann das verheerende Folgen für unsere moderne Gesellschaft haben. Maßnahmen zur Vorbeugung und Absicherung sind zeit- und kostenintensiv. Besonders für kleine und mittlere Unternehmen sind tragbare Wege erforderlich, um dieser Herausforderung gerecht zu werden. Managed Security kann ein Teil der Lösung sein.

Um gesellschaftlich wichtige ITK-Systeme, etwa im Bereich Mobilität, Energieversorgung und Finanzwesen, künftig verstärkt zu sichern, legte Bundesinnenminister Horst Seehofer im vergangenen Jahr einen Entwurf für das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) vor. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) soll als Hauptakteur im Kampf gegen Botnetze, Verbreiter von Schadsoftware oder vernachlässigte Geräte im IoT auftreten. Allgemein vernetzte Systeme rücken in den Fokus. Zudem soll ein neues Kennzeichen die IT-Sicherheit von Produkten sichtbar machen. Um industrielle Infrastrukturen zu schützen, bedarf es nicht nur technischer Sicherheitsmaßnahmen, sondern auch der Früherkennung.

Klassische Informationstechnologien wie IT (Hard- und Software, Netzwerktechnik et cetera) oder EDV (Programme zur elektronischen Datenverarbeitung wie Microsoft Office) und der OT-Bereich (Operational Technology, etwa zur Prozesssteuerung und Automatisierung) unterscheiden sich grundlegend in der Auslegung ihrer Kommunikation. Während sich herkömmliche IT auf Kommunikation und Vertraulichkeit fokussiert, sind in der Produktion insbesondere die Verfügbarkeit und Betriebssicherheit wichtig. Durch die Vernetzung von Prozessen verschmelzen IT- und OT-Umgebungen miteinander, etwa die Betriebs- und Steuertechnik.

Verglichen mit IT-Systemen für Bürokommunikation haben OT-Infrastrukturen oft eine längere Nutzungsdauer, müssen aber mit aktuellen Sicherheitsanforderungen mithalten können. So ist die Sicherheit von Hardware und Software längst ein wesentlicher Faktor bei der Entwicklung. Da qualitative Maßnahmen mit hohen Investitionen einhergehen und explizites Know-how erfordern, sind besonders kleine Unternehmen häufig überfordert. Damit sich die Anschaffung lohnt und Schutzprogramme richtig eingesetzt werden, spielen ein passgenaues Konzept und Usability eine wichtige Rolle.

Bedrohung hat viele Gesichter

Ob es um die Vorbeugung von Datendiebstahl, den Schutz vor Schadprogrammen oder Botnetzen geht – der Weg zur sicheren Infrastruktur muss präzise und bedarfsorientiert geplant werden. Lediglich eine kleine Sicherheitslücke oder ein Versäumnis beziehungsweise Fehler durch menschliches Versagen reichen aus, damit Hacker beispielsweise komplette Produktionssysteme oder Betriebsprozesse lahmlegen und auf diese Weise massiven Schaden anrichten können.

In seinem jährlichen Lagebericht zur IT-Sicherheit hält das BSI den aktuellen Stand der Cybersecurity in Deutschland fest. Produktionsausfälle, Beschädigungen von Maschinenparks, Patentdiebstahl oder Cybererpressung erhöhen die Dringlichkeit von passenden IT-Sicherheitsvorkehrungen. Das Thema Ransomware bleibt zentral: "Selbst wenn Backups erstellt wurden, entstehen den Unternehmen Schäden durch den Ausfall der verschiedenen Netze und Systeme, durch die Zeit der Wiederherstellung aus den Backups sowie durch die

Datenverluste aufgrund der Zeit zwischen der letzten Sicherung und dem Schadenseintritt." [1]

Gelingt es Schadsoftware, in Unternehmensnetze einzudringen, können Angreifer Zugangsdaten auslesen, sich selbstständig im Netz ausbreiten und Remotezugriff auf die Systeme erhalten. Die Schadprogramme werden ständig modifiziert, damit herkömmliche Virenschutzprogramme keine Chance haben, sie abzuwehren. "Bereinigungsversuche bleiben in der Regel erfolglos und bergen die Gefahr, dass Teile der Schadsoftware auf dem System verbleiben. Einmal infizierte Systeme sind daher grundsätzlich als vollständig kompromittiert zu betrachten und müssen neu aufgesetzt werden", so das BSI.

Deutscher Mittelstand im Visier

Angesichts der Veränderungen durch das verschärfte Sicherheitsgesetz stehen KMU nicht nur vor der Herausforderung, die (neuen) Vorschriften des Gesetzgebers und ihre eigenen, mit der Zeit wachsenden Anforderungen zu überblicken – sie müssen auch eine langfristige Sicherheitsstrategie entwerfen und umsetzen. Diese gesetzliche Anforderung trifft prinzipiell traditionelle Betreiber von kritischen Infrastrukturen sowie auch die Zulieferer.

Insbesondere mittelständische Unternehmen verfügen in ihrem Fachbereich über Spezialwissen und werden von Angreifern genauso ins Visier genommen wie größere Unternehmen. Ein Beispiel ist die erfolgreiche Attacke auf die Pilz GmbH, einen Spezialisten für Sicherheits- und Steuerungstechnik. Im Herbst 2019 verschafften sich Hacker Zugriff auf sämtliche Unternehmensserver, verschlüsselten die dort gelagerten Daten und forderten ein Lösegeld. Selbst die Firmenwebsite wurde in den Wartungsmodus versetzt.

Auch das große Chemieunternehmen Lanxess wurde über Jahre hinweg durch eine Hackergruppe mit dem Namen "Winnti" unbemerkt ausspioniert. Ein weiterer Fall ist der Elektronikkonzern Conrad, bei dem es vor wenigen Monaten zu einem Datenunfall kam: Angreifer verschafften sich über eine Sicherheitslücke Zugriff auf einen Teil des IT-Systems und somit auf rund 14 Millionen Kundendatensätze.

Fachkräftemangel: Managed Security als Ausweg

Viele Unternehmen haben bereits geeignete Schutzmaßnahmen umgesetzt. Im Rahmen des Lageberichts führte das BSI eine Cybersicherheitsumfrage durch, wonach mehr als zwei Drittel der befragten Institutionen ein strukturiertes Patchmanagement betreiben, um auf entdeckte Sicherheitslücken schnell zu reagieren. Betrachten wir große und kleinere Unternehmen getrennt, arbeiten etwa 70 Prozent der großen Unternehmen mit einem entsprechenden System, während nur knapp 40 Prozent der kleinen und mittelständischen Unternehmen ihre Geräte zentral verwalten – ein hohes Sicherheitsrisiko. Kam es in Folge dessen zu einem Angriff, ließ sich die Schwachstelle nicht mehr eindeutig ermitteln. Ziel von Schutzmaßnahmen sollte sein, dass die Manipulation eines Systems nicht die Übernahme des gesamten Netzes ermöglichen darf. Um dies sicherzustellen, bietet sich eine Kombination aus Detektions- und Präventionsmaßnahmen an.

Die Umsetzung einer geeigneten und langfristigen Sicherheitsstrategie bedarf interner Ressourcen und Fachwissen. Hier macht sich wiederum der Fachkräftemangel bemerkbar, denn insbesondere KMU können ihren Bedarf an Digitalkompetenz nicht decken. Mit einer aktuellen, repräsentativen Studie fand die staatliche Förderbank KfW heraus, dass ein Drittel dieser Unternehmen nicht genug Wissen über die digitale Transformation und die damit einhergehenden Herausforderungen hat. Besonders alarmierend sei die Situation bei komplexen Kenntnissen, etwa für Spezialsoftware. So benötigt fast die Hälfte der Mittelständler qualifizierte Datenanalysten.

Managed Security ist der richtige Ansatz für eine kosteneffiziente, zukunftsorientierte Sicherheitsstrategie. Mit der Unterstützung eines kompetenten Spezialisten können KMU ein erweiterbares, bedarfsorientiertes Konzept aufstellen und sich als vertrauenswürdige Geschäftspartner positionieren. So haben langjährige, qualifizierte Systemintegratoren umfangreiche Erfahrungen mit regulatorischen Verfahren und unterstützen Kunden von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung.

Skalierbare Sicherheit

Um das Risiko von Sicherheitslücken zu minimieren, sollten Infrastrukturen, Anwendungen, Clouds und Endgeräte kon-

tinuierlich überwacht werden. Bevor es an die Implementierung geht, müssen IT-Verantwortliche die Ausgangslage erfassen und Schwachstellen analysieren.

Eine Schwachstellenanalyse identifiziert Angriffspunkte sowohl in den technischen Anlagen als auch in den organisatorischen Prozessen eines Unternehmens und bestimmt den tatsächlichen Sicherheitsstand der IT- und Telekommunikationsinfrastruktur. Diesen Schritt sollte idealerweise ein externer Partner durchführen, denn dieser geht nicht nur systematisch vor, sondern ist auch unvoreingenommen. Zuerst werden die sicherheitsrelevanten Elemente der Infrastruktur und Abhängigkeiten festgelegt. Neben Interviews und Workshops zur Erfassung möglicher Gefährdungen in Gesamtprozessen erfolgt eine technische Prüfung, bevor die Erhebungen analysiert, Risiken klassifiziert, bewertet und dokumentiert werden. Ein weiterer Workshop thematisiert dann die Schwachstellen und erläutert einen Plan mit empfohlenen Korrekturmaßnahmen. Neben Schulung, optimierter Zutrittskontrolle, umfangreicherer Dokumentation et cetera helfen technische Maßnahmen, wie etwa ein isolierter Zugriff auf sensible Komponenten, Gefahren wirksam abzuwehren.

Vor Hackerangriffen schützen auch Maßnahmen zur Netzsegmentierung, Systemhärtung und Sandboxing. Sie wehren tiefergreifende Gefahren ab und schützen vor Sicherheitslücken, die beispielsweise durch Fehlverhalten von Mitarbeitern entstehen. Eine Netzsegmentierung unterteilt Unternehmensnetze in Bereiche, die so wenig wie möglich miteinander verbunden sind. Ein System zu härten heißt einfach ausgedrückt, zu definieren, wer auf welche Systeme und deren Unterbereiche zugreifen kann und wer nicht. Das gilt besonders für kritische Anwendungen, die in verschiedenen Sandboxes laufen sollten. Sandboxing bedeutet, eine Software oder einen Prozess innerhalb einer isolierten Laufzeitumgebung auszuführen. Das gesamte System ist in mehrere Sandboxes unterteilt, sodass das Betriebssystem und kritische Anwendungen getrennt voneinander laufen.

Insbesondere Steuerungsanlagen wie in Produktionsumgebungen haben oft einen langen Lebenszyklus und arbeiten daher mit veralteten Betriebssystemen, die Schwachstellen aufweisen. Gerade hier empfiehlt sich Sandboxing, ebenso für Workstations, Server, Cloudsysteme und ganze Data Center. Die Maßnahme ist für alle gängigen Betriebssysteme möglich und Angreifer beziehungsweise Schadprogramme können so nicht auf diese Bereiche zugreifen. Sandboxing schützt auch vor Zero-Day-Attacken, bei denen neue Sicherheitslücken ausgenutzt werden, bevor sie geschlossen sind.

Sicherheitsüberwachung mit SIEM und SOC

Lösungen für Managed Security umfassen SIEM-Tools, Supportleistungen für den Schutz von IT-/OT-Umgebungen und individuelle Lösungen für Multi-Vendor-Umgebungen. Dafür wählen Spezialisten wie die Firma telent einen fortschrittlichen Technologiemix aus Hard- und Software, maschinellem Lernen und Künstlicher Intelligenz (KI), um den Datenfluss lückenlos zu überwachen. Zahlreiche detaillierte Korrelationsinformationen und Algorithmen lösen Alarme aus und weisen auf potenzielle Gefahren hin.

Anomaly Detection (deutsch: Anomalie-Erkennung) ist eine weitere Möglichkeit der Absicherung. Ein solches System erkennt ungewöhnliche Vorgänge zeitnah und schlägt Alarm, etwa wenn ein Netzwerkgerät plötzlich ein anderes Kommunikationsprotokoll nutzt oder Datenverkehr ungeplant eine neue Route nimmt. Um eine Normabweichung festzustellen, erfasst das System zuerst den Normalzustand, indem es die IT-Architektur analysiert und im Hintergrund lernt.

Ergänzend zu technischen Lösungen empfiehlt sich ein Security Operation Center (SOC) – ein Expertenteam, das Netzwerke kontinuierlich überwacht, nach Bedrohungen sucht und sie entfernt. Ein effektives SOC aufzubauen, kostet einiges an Ressourcen und Zeit, weshalb sich zahlreiche kleine und große Unternehmen gegen eine eigene Funktion zur Sicherheitsüberwachung entscheiden und erfahrene Anbieter von Managed Security Services zu Rate ziehen.

Zu guter Letzt sollten Unternehmen etwa durch Awareness-Trainings und -Kampagnen die organisatorische Sicherheit bezüglich des Faktors Mensch erhöhen. Ein System zu härten bedeutet auch, nur die Komponenten einzusetzen, die für den Systembetrieb notwendig sind; denn es sind Menschen, die die Prozesse definieren und die Technologie kontrollieren.

Doch auch wenn Anwender alles richtig machen, kann sich beispielsweise über privat und geschäftlich genutzte portable Speichermedien wie USB-Sticks oder SD-Karten Malware einschleichen. Der Umgang mit Wechseldatenträgern sollte daher genau festgelegt werden, vor allem in sensiblen Umgebungen wie in Entwicklungsabteilungen oder Forschungseinrichtungen, aber auch in Verwaltungen. Ein Ansatz, der den Einsatz der mobilen Datenträger auf sichere Art ermöglicht, ist eine Datenschleuse. Ein solches System untersucht Wechseldatenträger, noch bevor sie mit einer sicheren Netzwerkumgebung in Berührung kommen. Wichtig ist, dass etwa auch Archivdateien auf den zu untersuchenden Medien miteinbezogen werden.

Fazit

ITK-Systeme sind weiterhin hochgradig gefährdet und benötigen besonderen, bedarfsgerechten Schutz. Essenziell ist die Kommunikation mit allen Beteiligten, denn nur so lassen sich die passenden Lösungen ausfindig machen und erfolgreich etablieren. Cybersecurity ist hier ein klarer Business Enabler. Als vertrauenswürdige Geschäftspartner aufgrund einer verlässlichen wie sicheren IT schaffen Unternehmen Innovation und Wachstum. Dienstleister können besonders kleinere Firmen dabei unterstützen. *(dr)*

Nico Werner ist Head of Cybersecurity bei der telent GmbH.

Link-Codes

[1] BSI: Die Lage der IT-Sicherheit in Deutschland 2019. S. 48ff.
k5zc1