Foto: Sergey Nivens - Fotolia

Wirkungsvolle Cybersecurity-Konzepte berücksichtigen sowohl den Faktor Mensch und die Organisation als auch die nötige Technologie.

# Plus an Netzwerksicherheit

## Schritte, um umfassende Netzwerksicherheit zu realisieren – von der Risikoanalyse bis hin zur Netzwerksegmentierung.

**DANIEL WEBER UND JAKOB SCHMIDT**

Wirkungsvolle Cybersecurity-Konzepte berücksichtigen bei der Netzwerksicherheit drei Säulen: den Menschen, Organisation und Prozesse und natürlich die Technologie – und zwar gleichermaßen. Das ist Konsens. Aber auch, wenn der technologische Part nicht herausragt und es schlicht und einfach unmöglich ist Cybersecurity nur über ihn abzubilden, nimmt er eine wichtige Stellung ein. Deswegen ist es in einer Welt, in der alle Bereiche des Lebens und die Arbeitswelt insbesondere in immer größerem Ausmaß von Informationstechnologie abhängen oder von ihr beeinflusst werden, ein gängiger Weg bei der Absicherung von IT- und OT-Netzwerken bei der Technologie einzusteigen. Doch wo anfangen bei der Absicherung des eigenen Netzwerks?

### Cybersecurity-Konzept auf Netzwerkebene

Bevor es überhaupt möglich ist ein Cybersecurity-Konzept auf Netzwerkebene umzusetzen, zu definieren, welche Maßnahmen sinnvoll sind und an welcher Stelle Handlungsbedarf besteht, müssen erst einmal die möglichen Bedrohungen identifiziert werden. Das sollte mittels einer aussagekräftigen Risikoanalyse erfolgen. In diesem Rahmen werden Risiken identifiziert und bewertet sowie ein Maßnahmenplan erarbeitet, der regelt, wie mit den erkannten Risiken umgegangen wird. Zusätzlich gehört zu einem vollwertigen Risikomanagementprozess die Überwachung, fortlaufende Überprüfung und ein Reportingsystem.

„Ein erster Schritt zu mehr Sicherheit ist es, eine Netzwerksegmentierung vorzunehmen. „

**Daniel Weber,** Teamleiter Security Solutions bei der Telent GmbH

### Kenntnisse über das jeweilige Unternehmensnetzwerk sind entscheidend

Bevor es aber überhaupt möglich ist die eigenen Risiken sinnvoll zu bewerten, gilt es die zu schützenden Werte und Assets zu bestimmen. Vereinfacht gesagt: Nur, wenn ich weiß, wie mein Netzwerk aufgebaut ist, welche Komponenten, Geräte und Zugänge vorhanden sind, kann ich überhaupt erkennen, wo mögliche Gefahren liegen. Daher empfiehlt es sich mit einer Netzwerkanalyse zu starten, denn die Erfahrung lehrt, dass in über Jahren gewachsenen Netzen viele Assets einfach nirgendwo bekannt, nicht verzeichnet sind. Hierfür ist es wichtig, spezialisierte Ansätze und dedizierte Services wie die K-Radar-Lösung von Koramis – Cybersecurity by

Telent zu nutzen. Mit solchen Ansätzen ist es möglich, Assets, Kommunikationsbeziehungen, Protokolle, Fehlkonfigurationen, Schwachstellen und vieles mehr zu identifizieren – ohne die operative Funktionalität von Netzwerkelementen und IT-Systemen zu unterbrechen. Netter Nebeneffekt: Am Ende steht ein aktueller Netzwerkplan zur Verfügung.

## Risikoanalyse: Wo lauern die Bedrohungen durch Cyberangriffe?

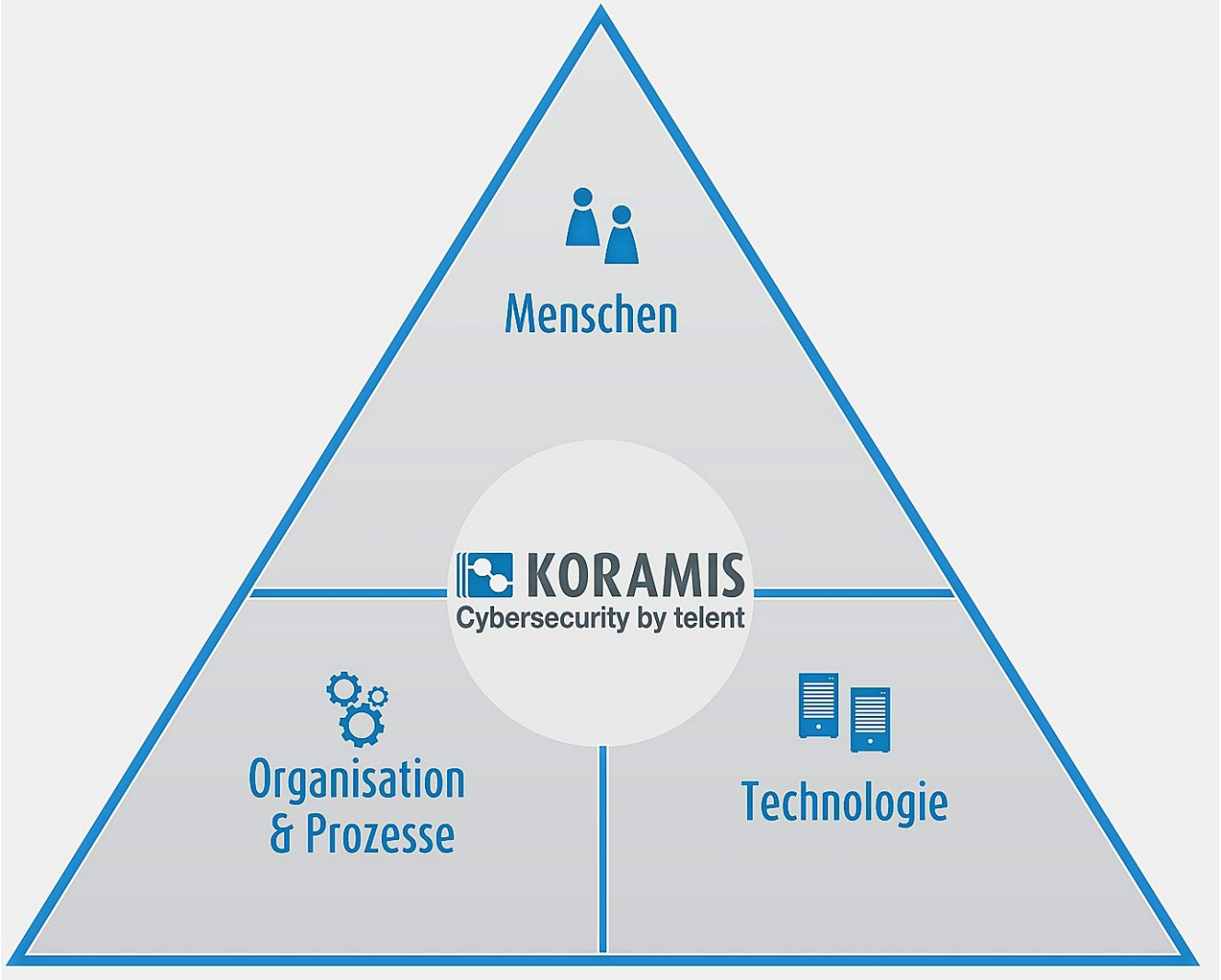
Im Anschluss ist es im Rahmen der Risikoanalyse möglich die Art der Bedrohung – also handelt es sich beispielsweise um das Einschleusen von Schadsoftware oder rührt sie von Social Engineering her – sowie die ursächlichen Schwachstellen zu bestimmen. Anhand einer standardisierten Risikomatrix, die Eintrittswahrscheinlichkeit und möglichen Impact bewertet, gilt es nun eine Risikoeinschätzung vorzunehmen und passende Gegenmaßnahmen einzuleiten.

Nachdem mit Hilfe der Netzwerkanalyse ein aktueller Netzplan vorhanden und dank der Risikoanalyse die Gefahrenpotentiale und schützenswerten Assets bekannt sind, gibt es ein paar grundlegende Maßnahmen, die das Security-Level erheblich steigern.

Ein erster Schritt zu mehr Sicherheit ist es eine Netzwerksegmentierung vorzunehmen. Dabei wird das Unternehmensnetz in kleinere „Netze“, sogenannte Zonen, aufgeteilt. Diese Zonen haben nur bedingt Zugriff untereinander, bzw. der Zugriff wird beispielsweise über Router oder eine Firewall reglementiert. Im Endeffekt sorgt die Segmentierung dafür, dass nur Geräte, die sich im selben Netzsegment befinden, miteinander kommunizieren können. Wollen Sie mit einem anderen Netzsegment kommunizieren, führt der Weg nur über eine Firewall. Diese entscheidet anhand der hinterlegten Regeln, ob diese Kommunikation erlaubt ist oder nicht.

## Leistungs- und Security-Aspekt

Einerseits sorgt eine solche Segmentierung für eine bessere Laststeuerung – sprich das jeweilige Segment ist in der Regel performanter. Viel wichtiger allerdings ist der Security-Aspekt. Dadurch, dass die Kommunikation der Segmente untereinander




Grafik: Telent

Die Faktoren Mensch, Organisation und Prozesse sind ebenso wie die Technologie im Sicherheitskonzept zu berücksichtigen – im Idealfall gleichermaßen


Grafik: Telent

Bei der Entwicklung und Umsetzung eines Cybersecurity-Konzepts sind mehrere wesentliche Schritte zu gehen.

reglementiert ist, können Sicherheitsvorfälle eingedämmt werden, die Gefahr, dass direkt das Gesamtnetz von einem Angriff betroffen ist, wird gebannt - die Angriffsfläche in Bezug auf besonders schützenswerte, betriebskritische Assets wird bedeutend verringert.

Wie die einzelnen Netzsegmente im Endeffekt ausgestaltet sind, ist dabei von den jeweiligen Anforderungen abhängig. Auf jeden Fall sinnvoll ist etwa eine Trennung des Office- vom Produktionsnetz. Schließlich gibt es keine Notwendigkeit, dass der Mitarbeiter in der Buchhaltung auf die Anlagensteuerung in der Produktion zugreifen kann oder der Maschinenbediener auf das Abrechnungswesen. Neben dieser groben Trennung empfiehlt sich eine weitere Segmentierung, etwa abteilungsweise oder hinsichtlich der Aufgabe.

Ein Produktivnetz sollte immer aus mehreren Netzsegmenten bestehen, die voneinander getrennt sind. Damit ist sichergestellt, dass im Falle eines Incidents nicht das komplette Netz betroffen ist und in seiner Gänze ausfällt. Der Datenfluss zwischen den einzelnen Segmenten sollte auf das notwendige Maß reglementiert sein und mit einer dezidierten Firewall überwacht und gesteuert werden. Unkontrollierte Verbindungen zu den Netzwerksegmenten sind zu unterbinden. Zudem kann, vor allem bei einem hohen Schutzbedarf einzelner Segmente, die Einführung einer Demilitarisierten Zone (DMZ) sinnvoll sein. Vereinfacht gesagt bildet eine solche DMZ ein Zwischennetz an den Netzübergängen, die zu keinem der beiden anderen Netze gehört.

Unbedingt sollte eine DMZ - sozusagen als Puffer - zwischen dem internen Netz und dem Internet stehen. Damit wird sichergestellt, dass Angreifer sich nach einer erfolgreichen Attacke nicht direkt frei im internen Netz bewegen können und die sensiblen Systeme angreifen kann.

## Zugriffsrechte der User und Gruppen

Im Zuge der Segmentierung sollten zudem die Zugriffsrechte der User und Gruppen festgelegt werden. Hierbei empfiehlt es sich einen Least-Privilege-Ansatz umzusetzen – also den verschiedenen Gruppen und Nutzern nur diejenigen Rechte zu gewähren, die diese auch tatsächlich benötigen. Der normale E-Mail-Nutzer braucht beispielsweise keinen Administratorenzugriff auf den Exchange-Server, um seine E-Mails bearbeiten zu können, der Maschinenbediener benötigt im Normalfall auch keinen Zugriff auf die gesamte Produktionsumgebung und Mitarbeiter müssen auch keine tiefergehende Rechte auf das Zeiterfassungssystem haben, um Stunden buchen zu können. Auch dadurch wird das Bedrohungspotential reduziert, da selbst wenn ein Angreifer Zugriff auf bestimmte Credentials hat, er erst einmal nur eingeschränkt agieren kann.

„Die schönste Topologie, die besten Firewalls und all die andere hervorragende Technik bringen allerdings wenig, wenn sie durch eine Vielzahl externer Schnittstellen, wie etwa im schlimmsten Fall undokumentierte Fernwartungszugänge, ausgehebelt werden."

**Jakob Schmidt,**
Coordinator Awareness Koramis bei der Telent GmbH

## Technik, Schnittstellen und Zugänge

Die schönste Topologie, die besten Firewalls und all die andere hervorragende Technik bringen allerdings wenig, wenn sie durch eine Vielzahl externer Schnittstellen, wie etwa im schlimmsten Fall undokumentierte Fernwartungszugänge, ausgehebelt werden. Daher – und hier kommt die schon erwähnte Netzwerkanalyse ins Spiel – sollten alle externen Schnittstellen dokumentiert werden. Im Anschluss gilt: weniger ist mehr. Wenn eine externe Schnittstelle nicht unbedingt notwendig ist, sollte sie deaktiviert werden. An Stellen, an denen dies keine Option ist, sollten diese über eine starke Authentisierung abgesichert werden. Zusätzlich müssen alle Verbindungen und Verbindungsversuche überwacht und protokolliert werden. Wenn Zugänge nur zeitlich beschränkt notwendig sind, sollten diese bei Nicht-Bedarf deaktiviert werden.

Wenn wir gerade beim Thema Kontrolle sind: Auch, wenn die Netzwerksegmentierung die Angriffsfläche verringert, es Angreifern erschwert sich unberechtigt Zugriff zu verschaffen, ist ein erfolgreicher Angriff natürlich nicht vollständig auszuschließen. Um solche Attacken zu erkennen, kann ein System zur Angriffserkennung eingesetzt werden, mit dessen Hilfe der Netzwerkverkehr innerhalb der verschiedenen Segmente überwacht und analysiert wird. Erkennt das System eine von der zu erwartbaren Kommunikation abweichendes Muster, schlägt es Alarm oder leitet Gegenmaßnahmen ein.

Zusammenfassend lässt sich feststellen, dass die geschilderten Maßnahmen – die sich natürlich zusätzlich zu dem vorhandenen Perimeterschutz verstehen – das Security-Niveau bedeutend heben, die Angriffsfläche erheblich verringern und im Falle einer erfolgreichen Cyberattacke dafür Sorge tragen, dass diese erst einmal nur begrenzt wirksam ist. ■

**telent GmbH:**
www.telent.de/de