Kommunikations-sicherheit

Das 13. Kapitel der ISO 27002 behandelt die Sicherheit in der Kommunikation. Das Ziel ist der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen sicherzustellen.

Zuerst gilt es das Netzwerk vor unbefugtem Zugriff zu schützen. So sollten Computer-Anschlüsse nicht auf Vorrat gepatcht werden, das heisst mit dem Netzwerk verbunden sein, sondern nur bei Bedarf. Technisch kann das Protokoll 802.1x eingesetzt werden. Nur bekannte Geräte bekommen eine IP-Adresse. Alternativ können nicht bekannte Geräte in ein Gast-Netzwerk verbunden werden. So können diese mit dem Internet kommunizieren, erreichen aber keine Firmen-Systeme. Die Identifizierung kann anhand der MAC-Adresse (eindeutige Adresse der Netzwerkkarte) oder über Zertifikate erfolgen. Beide haben ihre Vor- und Nachteile.

Verantwortlichkeiten trennen

Weiter gilt es entsprechende Verantwortlichkeiten und Verfahren zu definieren. Idealerweise werden die Verantwortlichkeiten getrennt: jemand ist für die Systeme (Server, Clients, usw.) zuständig, eine andere Person für das Netzwerk (Anschlüsse, IP-Adressen, Internet-Zugang, Firewall, Switch-Konfiguration usw.). Die Netzwerkelemente müssen ebenfalls überwacht werden. Diese können in das vorhandene Log-System integriert werden (siehe Maschinenbau 6/19). Praktisch alle Geräte kommunizieren über das SNMP-Protokoll (Simple Network Management Protocol) mit diesem Log-System. Ausfälle und Abweichungen können per E-Mail oder SMS an die verantwortliche Person geschickt werden. Dazu sind die Verfügbarkeiten im Vorfeld zu definieren. Wie lange dürfen ein System oder eine Netzwerk-Komponente ausfallen? Bei externen Dienstleistern sind diese Werte in die Vereinbarung aufzunehmen. Doch alle Daten nützen nichts, wenn diese nicht regelmässig ausgewertet werden. Dies gehört zu den täglichen Aufgaben des Netzwerk-Verantwortlichen.

Eine wichtige Voraussetzung ist das Auftrennen der Netzwerke. Dazu wird eine Firewall eingesetzt. Mit mehreren Netzwerkkarten ausgerüstet, können unterschiedliche Anforderungen an Netzwerke eingerichtet werden. Klassischerweise unterscheidet man zwischen Internet, DMZ und Intranet. In die DMZ gehören Systeme, welche vom Internet her erreichbar sind, wie E-Mail-, Web- oder FTP-Server. Immer mehr setzen sich aber auch Mikronetzwerke durch, das heisst Systeme werden noch genauer auseinandergehalten. So kommen schnell viele Netzwerksegmente zusammen. Dank Virtualisierung kann auch die Firewall so betrieben werden, es ist keine zusätzliche Hardware mehr notwendig. Als weitere Möglichkeit kommen VLANs zum Einsatz. Hier werden unterschiedliche Netze über das gleiche Kabel übermittelt. Es ist damit keine physische, sondern eine logische Trennung. In den IP-Paketen wird die VLAN-Nummer mitübertragen und kann anders geleitet werden. Für weniger kritische Netzwerkzonen eine einfache und schnelle Möglichkeit der Trennung.

Regeln im Umgang mit Anrufbeantwortern und Fax-Geräten

Der zweite Teil hat zum Ziel, die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, aufrecht zu erhalten. Dazu gehören Verfahren, um das abfangen, kopieren, verändern, umleiten oder zerstören zu verhindern. Eine Möglichkeit ist die Nutzung der Verschlüsselung (siehe dazu Maschinenbau 4/19). Damit kann ein Teil, aber nicht alle, Anforderungen erfüllt werden. Wie auf den Endgeräten sollten Antivirenprogramme zum Schutz vor Malware verwendet werden. Viele Anbieter haben dies in die Firewall integriert und scannen so jedes Paket, das durchfliesst. Neben den technischen Möglichkeiten gilt es eine Weisung zur Datenübertragung zu erstellen. Dies kann beispielsweise in der Klassifizierung von Informationen erfolgen (siehe dazu Maschinenbau 3/19).

Darin gilt es auch Anforderungen an E-Mails zu definieren. Was darf wie verschickt werden? Dürfen E-Mails an eine weitere Adresse weitergeleitet werden? Steht keine E-Mail-Verschlüsselung zur Verfügung, sollten mindestens die vertraulichen Daten verschlüsselt sein, zum Beispiel mittels ZIP. Die Norm verlangt weiter Regeln im Umgang mit Anrufbeantwortern und Fax-Geräten. Wie sind diese Geräte zu nutzen? Was darf damit übertragen werden?

Der dritte Teil umfasst Vereinbarungen zwischen der eigenen Firma und externen Parteien. Die Details dazu wird das Thema in der übernächsten Ausgabe sein. Auf technischer Seite sind dies die Definition der Verantwortlichkeiten, zum Beispiel für die Konfiguration der Geräte, Überwachung

Bild: Archiv

Schutz der Daten im eigenen Netzwerk.

und Alarmierung. Welche Verschlüsselungsverfahren gelten als sicher und werden verwendet? Bei der Übertragung per E-Mail gilt es die korrekte Adressierung sicherzustellen. Wem ist es nicht schon mal passiert, dass das E-Mail-Programm mit der Autovervollständigung einen falschen Empfänger ausgewählt hat. Auch gehört die Definition der elektronischen Signatur dazu. Welche Anforderungen daran gilt es einzuhalten?

Anforderungen müssen definiert werden

Dürfen auch öffentliche Dienste zur Datenübermittlung eingesetzt werden? WhatsApp ist zu einem ständigen Begleiter geworden. Doch ist er genügend für Business-relevante Anforderungen? Vermutlich nicht in allen Bereichen. Auch Slack kann immer mehr angetroffen werden. Jedes Unternehmen sollte Anforderungen an diese Dienste definieren. Wann darf welches Tool verwendet werden? Welche Informationen dürfen und welche dürfen eben nicht darüber übermittelt werden?

Weiter gilt es die Nachverfolgbarkeit und die Nichtabstreitbarkeit zu regeln. Doch Daten können nicht nur elektronisch übermittelt werden, sondern auch physisch. Wie muss die Information, zum Beispiel auf einem USB-Stick eingepackt sein? Muss das Paket eingeschrieben sein? Kommen Kurierdienste zum Einsatz? Wer haftet bei Verlust?

Bei jeglicher Kommunikation gilt es die Vertraulichkeit- und Geheimhaltung zu vereinbaren. Diese ist abhängig von der Kritikalität der übertragenen Daten und der Dauer. Diese Vereinbarungen gilt es regelmässig zu überprüfen und bei Veränderungen anzupassen. Was geschieht am Ende der Business-Beziehung mit den Daten? Sind diese zu löschen? Auch das gehört in die Vereinbarung. Vergessen werden darf auch das Recht zur Überprüfung und Überwachung der Aktivitäten. Was ist erlaubt? Was ist verboten? In die Vereinbarung gehören auch allfällige Drittparteien wie Sub-Lieferanten. Die gesamte Lieferkette gilt es sicherzustellen. Idealerweise bereits vor der Vertragsabschliessung, um unerwünschte Überraschungen zu vermeiden.

Mit diesen Regeln kann der Schutz der Daten sowohl im eigenen Netzwerk, wie auch bei der Übermittlung durch das Internet zu weiteren Stellen sichergestellt werden. Neben den technischen Vorgaben zum Schutz der Daten gilt es die vertraglichen Anforderungen schriftlich zu definieren und festzuhalten. Damit kann die Sicherheit der Daten vor, während und nach dem Transport garantiert werden.

INFOS | KONTAKT
goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen
T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch