ISO 27032 – Cybersicherheit

Cybersicherheit ist heutzutage ein Schlagwort geworden. Es reicht nicht mehr IT-Sicherheit oder Informationssicherheit umzusetzen, sondern die Gesamtheit wird mit Cyber adressiert. Bereits 2012 wurde von ISO eine Norm genau zu diesem Thema veröffentlicht. Zeit also, diese etwas genauer zu betrachten.

Im Vorwort geht die ISO-Norm genau auf dieses Thema Cyber ein und bezeichnet den Cyberspace als eine komplexe Umgebung, die sich aus der Interaktion von Menschen, Software und Diensten im Internet, unterstützt durch weltweit verteilte physische und virtualisierte Geräte und verbundene Netze. Es gibt jedoch Sicherheitsprobleme, die nicht durch die derzeitigen Sicherheitsverfahren nicht abgedeckt sind. Gerade bei Cloud-Diensten, die von verschiedenen Anwendern genutzt werden, ist nie klar, was alles ausgeführt, gespeichert und verarbeitet wird.

Schutz der Systeme

Die ISO 27032 wurde am 15. Juli 2012 veröffentlicht und trägt den Titel «Information technology – Security techniques – Guidelines for cybersecurity». Die Norm geht insbesondere auf die Schwerpunkte Social-Engineering-Angriffe, Hacking, Malware, Spyware und andere potenziell unerwünschte Software ein. Sie bietet in der Folge Leitfäden zur Vorbereitung auf Angriffe, zur Aufdeckung und Überwachung von Angriffen und wie auf Angriffe reagiert werden kann. Der zweite Schwerpunktbereich dieser internationalen Norm ist die Zusammenarbeit durch einen effizienten und effektiven Informationsaustausch.

Insbesondere nimmt die Norm auch Bezug auf kritische Infrastrukturen. Dazu zählen unter anderem die Energiebrache, Lieferketten, aber auch das Gesundheitswesen.

Blicken wir etwas genauer in die Norm hinein: In Kapitel 4 werden 53 Begriffe erklärt. Dies ist im Vergleich zu anderen Normen eher die Ausnahme, dass so viele Begriffe erläutert werden. Dazu gehören beispielsweise Adware, Avatar, Angriffspotenzial, Bot, Cookie, Cyberkriminalität, Cyberspace, Hacken, Internet, Malware, Phishing, Spam, Spyware, trojanisches Pferd, virtuelle Währung, Schwachstelle und Zombie. In Kapitel 5 folgen 29 Abkürzungen, die in der Norm genutzt werden. Auch dies ist eher untypisch, aber praktikabel, da Platz gespart wird und damit auch die Kosten beim Kauf geringer ausfallen. Normen werden jeweils nach Anzahl Seiten berechnet.

In Kapitel 6 wird eine Einführung zur Sicherheit im Internet und Cyberspace (die Natur des Cyberspace und das Wesen der Cybersicherheit) gegeben und es werden die Informations-, Anwendungs- und Netzwerksicherheit definiert. Auch wird die Sicherheit bei kritischen Infrastrukturen erläutert: «Die CIIP befasst sich mit dem Schutz der Systeme, die von Anbietern kritischer Infrastrukturen wie Energie-, Telekommunikations- und Wasserbehörden bereitgestellt oder betrieben werden. Die CIIP sorgt dafür, dass diese Systeme und Netze gegen Risiken der Informationssicherheit, der Netzsicherheit, der Internetsicherheit und der Cybersicherheit geschützt und widerstandsfähig sind.» (Quelle ISO 27032, Kapitel 6.3, Seite 11, eigene Übersetzung) CIIP steht dabei für critical information infrastructure protection, zu Deutsch Schutz kritischer Informationsinfrastrukturen.

Lösungen zum Schutz vor Angriffen

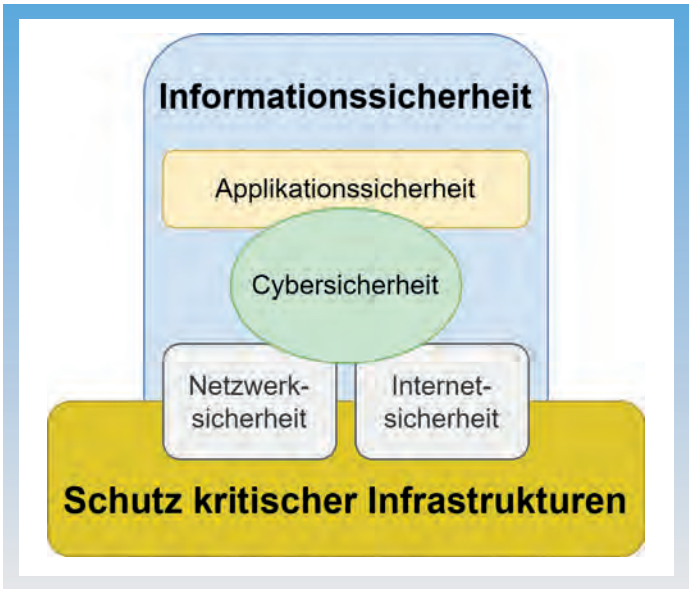
Spannend in diesem Kapitel ist auch die Beschreibung des Zusammenhangs zwischen Stakeholder (interessierte Kreise, wie Kunden, Lieferanten, Partner, Verwaltungsrat, Mitarbeitende, usw.), Schwachstellen, Massnahmen, Risiken, Werten und Hackern. In einer Grafik werden die verschiedenen Beziehungen aufgezeigt und beschrieben.

In Kapitel 6.5 wird die Vorgehensweise zur Bewältigung von Cybersicherheitsrisiken erläutert. Dazu gehören Branchenpraktiken, die Zusammenarbeit aller Beteiligten, umfassende Awareness, zuverlässige Quellen für die Erkennung und Bewältigung von Cybersicherheitsrisiken sowie innovativer technischer Lösungen zum Schutz vor Angriffen. Die Anleitungen beschreiben Rollen, Richtlinien, Methoden, Prozesse und technische Kontrollen.

Weiter werden in Kapitel 7 die beiden Interessensgruppen kurz beschrieben, in Kapitel 8 folgen die (Vermögens-) Werte (Personal und Organizational assets) sowie in Kapitel 9 die Bedrohungen und Schwachstellen dieser Werte. Es wird dabei zwischen Angriffen aus dem internen Netzwerk und aus dem Internet unterschieden. Bei beiden Arten werden mehrere Beispiele gegeben. In Kapitel 10 folgen dann noch die beteiligten Rollen: verschiedene Individuen, in einer Organisation sowie die Rolle des Providers.

Schutz von Server und Endgeräten

Einen grossen Teil nimmt das Kapitel 11 mit dem Titel Leitlinien für Interessensgruppen ein. Darin werden die drei Bereiche Sicherheitshinweise, internes Risiko-Management (mit Referenzen zur ISO 31000 und ISO 27005) und



Beziehung zwischen den Sicherheitsthemen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Sicherheitsanforderungen adressiert. Die Leitlinien für Organisationen und Dienstleistungsanbieter beinhaltet die Verwaltung der Unternehmens-Informationssicherheitsrisiken, die Bereitstellung von sicheren Produkten, der Netzwerküberwachung inkl. Reaktion auf Vorfälle, Unterstützung und Eskalation, der Aktualität von Information und Sicherheitsanforderungen für das Hosting von Web- und anderen Cyberanwendungen. Hinweis: Mehr über das Risiko-Management finden Sie in der Ausgabe Maschinenbau 2018/8 Risikomanagement.

Nach der Bewertung der Risiken folgen in Kapitel 12 die Kontrollen. Dazu gehören Kontrollen auf der Anwendungsebene, der Schutz von Server und Endgeräten (zum Beispiel aktuelle Betriebssysteme, unterstützte Software-Anwendungen, die Verwendung von Antiviren- und Antispyware-Tools, aktivieren von Skript-Blockern, Phishing-Filter, Nutzung von Sicherheitsfunktionen und Firewall inkl. HIDS (hostbasiertes Erkennungssystem) sowie automatische Updates), Kontrollen gegen Social-Engineering-Angriffe, Erstellung von Richtlinien zu den Themen Kategorisierung und Klassifizierung von Informationen, Sensibilisierung und Schulung sowie Audit.

In Kapitel 13 folgen die Anforderungen für den Informationsaustausch und die Koordinierung, Methoden und Verfahren (zum Beispiel Geheimhaltungsvereinbarungen, Tests und Übungen sowie Zeitplan), Menschen und Organisationen (Allianzen, Sensibilisierung und Schulung) sowie die Anleitung zur Umsetzung. Im Kapitel Technik werden die Datenstandardisierung und Visualisierung, kryptographischer Schlüsselaustausch, Software-/Hardware-Backups, der sichere Datenaustausch sowie Prüfsysteme beschrieben.

In Anhang A wird auf die Überwachung des Darknets eingegangen (als Erinnerung: die Norm ist aus dem Jahr 2012, sie war also der Zeit etwas voraus), in Anhang B diverse Hinweise zur Online-Sicherheit und zum Schutz vor Spyware und eine Musterliste der Ansprechpartner für die Eskalation von Vorfällen gegeben sowie im Anhang C Beispiele für verwandte Dokumente (ISO und ITU-T) genannt.

Auch wenn die Norm schon zehn Jahre alt ist, hat sie an Aktualität nichts verloren. Auf 58 Seiten wird das Thema Cybersicherheit von verschiedenen Seiten beleuchtet. Es werden Gefahren, aber auch Massnahmen aufgezeigt. Als Lektüre und natürlich als Schutz vor einem möglichen Vorfall ist sie sehr zu empfehlen.