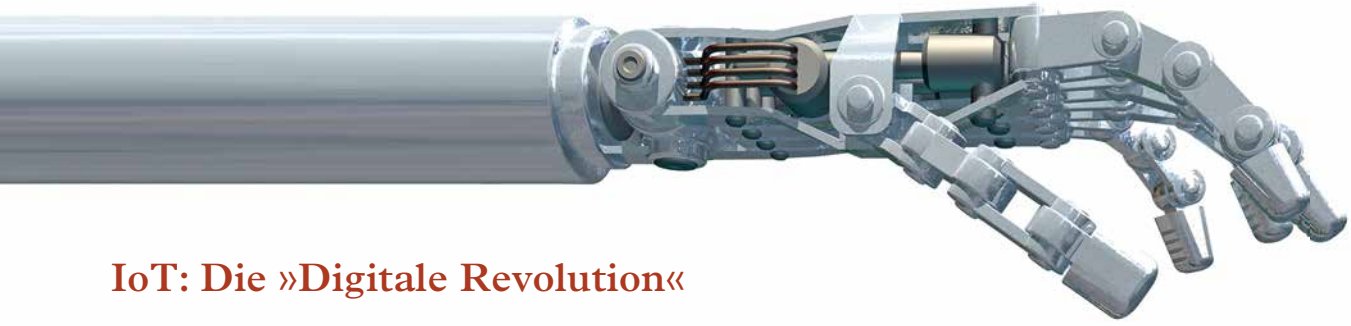
Heft 11-12, November-Dezember 2016 | 14. Jahrgang

manage it

IT-Strategien und Lösungen

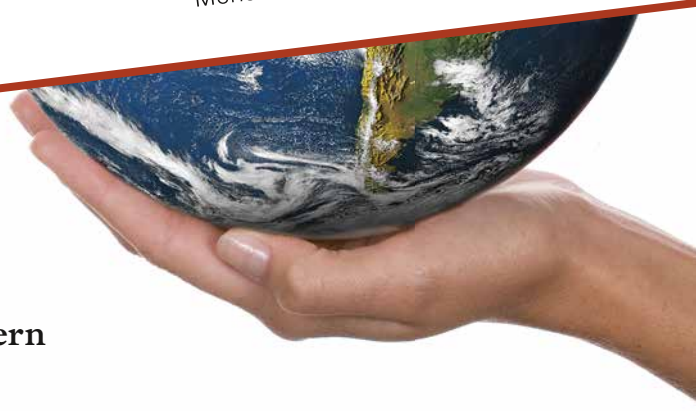
Digitale Transformation

IT-Strategie – neue alte Perspektiven



IoT: Die »Digitale Revolution«

Das Internet der Dinge



IT-Sicherheit

Social Engineering auf C-Level-Niveau verhindern

Security gepaart mit Backup und Recovery

IAM-Systeme im Vergleich

Remote Access und Security bei IoT

Cyber Security mit Augenmaß

Auf Planung und Organisation kommt es an

Illustration: © alphaspirit/shutterstock.com

Durch die digitale Transformation und das Internet der Dinge verstärken sich die Angriffsszenarien. Cyber Security muss holistisch und strukturiert geplant werden um die volle Wirkung zu entfalten.

Cyber Security hat viele Facetten. Die Angriffspunkte, um Daten, Geschäftsprozesse und Mitarbeiter in Mitleidenschaft zu ziehen, sind vielfältig. Demzufolge ist auch das Projekt ehrgeizig. Es geht darum, auf die mit der digitalen Transformation einhergehenden veränderten Bedrohungsszenarien die richtigen Antworten zu finden und Daten, Geschäftsprozesse und Akteure vor der Infiltration immer intelligenterer Malware sowie vor gezielten Angriffen von Cyberkriminellen zu schützen. Das funktioniert nur über eine kompetente und ganzheitliche Planung, die alle Wechselwirkungen zwischen den Projektphasen berücksichtigt.

Doch wie das Gesamtvorhaben Cyber Security mit klarem Blick, ganzheitlich und wohl koordiniert und strukturiert planen? Das hohe Ziel: Eine angemessene Planung mit Fokus auf ein umfassendes IT-Management, das Information Security Management System (ISMS) einschließt. Der Werdegang der anzustrebenden Cyber-Security-Lösung führt über die Phasen »Konzeption«, »Prozesse«, »Methoden/Technologien« und »Management des kulturellen Wandels«, wobei alle Wechselwirkungen zwischen den Phasen im Sinne eines in sich geschlossenen Kreislaufs hinreichend bedacht und bewertet werden müssen.

Konzeption. Am Anfang des Projekts steht die Identifikation der Handlungsfelder und Maßnahmen im Spannungsfeld zwischen notwendiger und leistbarer Cyber Security. Das IT-Sicherheitsgesetz des Bundesamts für Sicherheit in der Informationstechnik (BSI) liefert dafür konzeptionell den IT-Grundschutz, indem es je nach Branchenzugehörigkeit des Unternehmens Mindestsicherheitsstandards sowie Vorgehensweisen und Templates für die Konzeptionsphase beisteuert. Weitere, wertvolle Planungsorientierung eröffnen ISO-Normen, ISMS-Audits, Penetrationstests, Secure Development Lifecycles, Maßnahmen zur Netzwerksicherheit (u.a. Segmentierung und der Einsatz standardisierter Kommunikationsprotokolle). Alle diese Handlungsfelder und Maßnahmen müssen in der Konzeptionsphase durchdrungen, entworfen, festgelegt und dokumentiert werden. Eine besondere Bedeutung kommt den Penetrationstests zu. Nur im Wissen um die Schwachstellen kann später analysiert werden, welche davon für das Unternehmen tolerabel sind, also vernachlässigt werden können, und welche aufgrund der potenziellen Auswirkungen auf Daten, Geschäftsprozesse und Mitarbeiter behoben oder zumindest eingegrenzt werden sollten.

Prozesse. ISMS-Audits, Penetrationstests und Secure Development Lifecycles bedürfen Prozesse, um sie in Gang zu setzen. Diese Prozesse müssen ebenfalls entworfen, festgelegt und dokumentiert werden. Penetrationstests und ein davon abgeleitetes Risikomanagement zum Ausschluss beziehungsweise zur Minimierung der wichtigsten Risiken wird sich nur dann als für das Unternehmen wirtschaftlich erweisen, wenn das bestehende Sicherheitsniveau evaluiert wird. Nur unter dieser Voraussetzung können die für das angestrebte Maß an Cyber Security erforderlichen Aufwendungen und Investitionen in Methoden und Technologien genau bestimmt und exakt beziffert werden. Auch diese Evaluierung setzt die Einrichtung konkreter Prozesse voraus, die gestaltet, festgelegt und dokumentiert werden müssen. Auch eine kontinuierliche Berichterstattung (Reporting) und ein sicheres Design für die Infrastruktur und Anwendungsprogrammierung lebt förmlich von der Definition und Einrichtung konkreter, weitgehend automatisierter Prozesse. Dies ist auch für die kontinuierliche Verbesserung der Prozesse notwendig. Darüber hinaus sollten IT-Prozesse durch Automatisierung stringent gestaltet, insgesamt Cyber Security durch entsprechende organisatorische und technische Prozesse unterlegt werden, um die Effizienz, Effektivität und Wirksamkeit der Abwehr bei möglichst geringem Mitteleinsatz zu steigern.

Eine durchgehend stringente Prozessgestaltung ist schon deshalb wich-

tig, weil sie entscheidend für die Kontinuität der Internetgeschäfte, die Leistbarkeit und Flexibilität des Cyberschutzes sowie die Akzeptanz der Schutzmaßnahmen und -vorkehrungen unter den Mitarbeitern ist. Nur unter diesen Voraussetzungen:

- wird die Überwachung und Durchführung permanent auf hohem Niveau erfolgen,
- werden sich die personellen und finanziellen Aufwendungen in Grenzen halten,
- wird eine hohe Skalierbarkeit des Cyberschutzschirms erreicht werden,
- wird das IT-Personal durch weitgehend automatisierte Prozesse von umständlichen und fehleranfälligen Routinen entbunden werden.

Methoden und Technologien. Ebenso wie für die Konzeption von Cyber Security sind ISO-Normen, IT-Grundschutz nach BSI, Netzwerksicherheit, ISMS-Audits und Penetrationstests für die dritte Planungsphase, die Auswahl von Methoden und Technologien, essenziell. Sie steuern dafür geeignete Methoden bei. Zu diesen planungsunterstützenden Methoden gehören auch die von BSI zertifizierten Audits und die Reporting-Prozesse, die innerhalb der Phase »Prozesse« herausgebildet worden sind. An Technologien für Cyber Security mit Augenmaß stehen Identity and Access Management (IAM), Security Information and Event Management (SIEM), Threat and Malware Detection/Prevention, die technischen Mittel für Application Security und, mit Blick auf eine weitergehende Netzwerksicherheit Scanner wie Nessus oder OpenVas zur Verfügung.

Genauer betrachtet untergliedern sich die Handlungsfelder »Netzwerksicherheit« und »Application Security« in mehrere Methoden und Technologien, die für den späteren Einsatz durchdrungen, bewertet und festgelegt werden müssen:

- Secure Network Design
- Secure Remote Access-Technologien
- Security Enterprise Architecture-Management
- Security allgemein
- Microsoft Security
- Secure Application Development
- Application Penetration Testing
- General Access and Rights Concept

Cyber Security für Cloud-basierende Infrastrukturen und Anwendungen inklusive. Bestimmte Infrastrukturen und Anwendungen wird das Unternehmen künftig extern innerhalb von Clouds betreiben lassen wollen. Für die Öffnung der Geschäfte via Internet bietet sich diese Strategie für Unternehmen an, ebenso aus Kosteneinsparungsgründen. Welche Infrastrukturen und Anwendungen mit Blick auf Cyber Security nach draußen gegeben werden können, dies sollte bereits ausgehend von der Konzeptionsphase gründlich mit allen Vor- und Nachteilen (Risiken) analysiert werden. Für diese Infrastrukturen und Anwendungen müssen anschließend als Anforderungsprofil Prozesse, Strukturen und Verantwortlichkeiten definiert und festgelegt werden. Nur so kann später im Tagesbetrieb ein weitgehend nahtloses Zusammenspiel von internen und externen Kräften und Prozessen umgesetzt werden. Dazu sollten im nächsten Projektschritt auch die Methoden und Technologien gehören, deren Einsatz das Unternehmen auf Seiten der Cloud Provider für einen weitgehend sicheren gemeinsamen Internetauftritt erwartet. Außerdem sollte definiert, festgehalten und dokumentiert werden, welche Maßnahmen künftig durchgeführt werden sollten, um den Cyber-Security-Schutzschirm flexibel neuen Bedrohungssituationen anpassen zu können und welche Leistungen dazu die einzelnen Cloud-Dienstleister innerhalb ihrer Domäne überprüfbar und somit nachweislich erbringen müssen.

Nachhaltiges Management des kulturellen Wandels. Trotz weitgehender Automatisierung von Prozessen und dem Einsatz geeigneter Methoden und Technologien für mehr Cyber Security: Von den Menschen – IT-Personal, Mitarbeitern und Management – wird es weiterhin abhängen, welche Qualität der Schutzschirm und die Gegenmaßnahmen zur Abwehr von Malware und anderer Angriffe haben werden und ob alle Akteure die Cyber-Security-Strategie hinreichend akzeptieren und befolgen werden. Die Herausforderung besteht darin, allen Akteuren die mit der digitalen Transformation einhergehenden veränderten Bedrohungsszenarien nahezubringen, damit die sie verinnerlichen und angemessen auf diese Bedrohungen reagieren können. Das ist bei neuen Angriffsformen wie APT-Programmen besonders schwierig, die im Schnitt über zweihundert Tage passiv bleiben, bevor ihr Schadcode aktiv wird. Die vielen veränderten Bedrohungsszenarien kommen einem kulturellen Wandel gleich, der unternehmensintern nachhaltig gemanagt werden muss. Die Sicherheits- und Geschäftsstrategie, das Risikomanagement mit akzeptablen und nicht akzeptablen Bedrohungen sowie die ISMS-Strategie und das Berichtswesen müssen an die veränderte Gefahrenlage angepasst werden. Zudem muss unter den Akteuren die Sensibilität für die wichtigsten Gefahren durch Schulungen des IT-Personals, der Mitarbeiter und Führungskräfte geweckt und geschärft werden.

Carsten Triebel

» **Die Herausforderung besteht darin,** allen Akteuren die mit der digitalen Transformation einhergehenden veränderten Bedrohungsszenarien nahezubringen. «

Carsten Triebel
ist Senior Consultant
beim Beratungshaus
BridgingIT.