funkschau.de

funkschau

business.technology.strategy

KUNDENANSPRACHE 4.0
Neue Services, neue Potenziale

TK-ANLAGEN
Cloud vs. On-Premise

SECURITY
Von Back-up bis MDM

IOT
Produktdesign in der digitalen Welt

20
2016
28. Oktober
€ 6,00 sfr 10,00

Sonderdruck zum Thema
„Cybersecurity"

bridging IT
Menschen Methoden Lösungen

DER DIGITALE KUNDE

RISIKEN UND ABWEHR IN DER WAAGE

In dem Maße, wie sensible Daten über den Tellerrand des eigenen Unternehmens hinaus verteilt werden, müssen auch die Sicherheitsvorkehrungen ausgedehnt werden. Dennoch soll die Gesamtkonstruktion für mehr Sicherheit im Cyberspace für das Unternehmen leistbar sein und bleiben.

Autor: Carsten Triebel Redaktion: Markus Kien

Bild: fs Quelle: 12317

➤ Die Technologien, mit denen Daten aus der sicheren Obhut des Unternehmens nach draußen verteilt werden, hat viele Namen: Big Data, Virtualisierung, Cloud-Computing, Federation, Industrie 4.0, IoT, Mobile Business oder Social Networking. Der Preis, um über diese Techniken die digitalen Geschäfte voranzutreiben: immer mehr Angriffsflächen, die Angreifer aus dem Cyberspace für ihre zudem immer ausgefeilteren Attacken nutzen können. Gleichzeitig steht weiterhin die Infrastruktur mit den vitalen IT-Ressourcen des Unternehmens im Fokus der Kriminellen.

Die Herausforderung angesichts dieses Bedrohungsszenarios heißt: Sicherheitsvorkehrungen und -maßnahmen etablieren, die über den Perimeter-gestützten Schutz der eigenen Inhouse-IT-Infrastruktur und an den Netzwerkeingängen hinausgehen – die installierten Anti-Viren-Programme und Lösungen für Endgeräte-Sicherheit eingeschlossen. Dabei dürfen die Maßnahmen weder das IT-Budget sprengen noch die Geschäftsmodelle einengen.

Gefahren aus dem Cyberspace

Markt- und Technologiekenner haben klare Vorstellungen davon, durch welche neuartigen Attacken aus dem Cyberspace die größten Gefahren drohen: Das sind Kampagnen, die auf Vektoren aufsetzen und die Klick-Bereitschaft der Benutzer

FRAMEWORKS UND RICHTLINIEN ALS ORIENTIERUNGSHILFE

➤ Das Wissen um die Risiken und ihre potenziellen Folgen können für ein Assessment – sowie darauf aufbauend zum (Um-)Setzen realistischer und finanziell vertretbarer Sicherheitsziele – Frameworks oder Richtlinien herangezogen werden. Solche unterstützenden Frameworks und Richtlinien steuern unter anderem bei:

- ➤ Bundesamt für Sicherheit in der Informationstechnik (BSI),
- ➤ National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity,
- ➤ SANS/Council on Cybersecurity sowie
- ➤ Allianz für Cyber-Sicherheit.

Danach werden sowohl der Status quo in punkto Cybersecurity als auch die notwendigen Schritte, um diese zu verbessern, klarer.

ausnutzen. Angriffe mit einfach über das Internet beziehbaren Standard-Malware-Tools sind eine weitere Bedrohung aus dem Cyberspace. Solche Attacken können nicht von Signatur- oder Reputations-basierenden Sicherheitssystemen erkannt werden. Sie erweisen sich ohne geeignete Gegenmittel zudem als resistent gegenüber Analysen, Daten-Exfiltrationen und Selbstlöschungen. Insbesondere durch Standard-Tools, die sich APT-Methoden (Advanced Persistent Threats) bedienen, ist die Gefahr für Unternehmen, Opfer von Malware zu werden, erheblich gewachsen.

Mittels Advanced-Threat-Kampagnen können Anmeldedaten von Benutzern ausgespäht werden, ähnlich wie bisher bei Banken und Finanzinstituten. Massenkampagnen, die mit ihrer Methodik auf Benutzer abzielen, sind eine weitere gefährliche Bedrohung. Sie nutzen beispielsweise einen URL-basierenden Vektor, um vorbei an klassischen Analysatoren über Traffic Direction-Systeme (TDS) oder Exploit-Kits über die Benutzerschnittstellen Kerndaten oder Payloads abzuziehen. Mobile Anwendungen, die sich in offiziellen App-Stores abgelegter Malware bedienen, werden zunehmend dazu genutzt, diesen Schadcode in die IT-Infrastruktur des Unternehmens einzuschleusen. Dort wird die Malware einige Zeit schlummern, bevor sie aktiv wird und Benutzerdaten oder sonstige Kerndaten entzieht, Login- und Anmeldedaten ausspäht, SMS-Nachrichten abfängt oder Audio- und Videoerfassungssequenzen abgreift.

Über das Einführen betrügerischer Social-Media-Konten wird Malware infiltriert oder es werden fremdgesteuert Fälschungen, Raubkopien oder sonstige unrechtmäßige Produkte über den Social-Media-Auftritt des Unternehmens vertrieben. Zudem können Angreifer über betrügerische Social-Media Accounts Kunden- und Finanzdaten abziehen, sogar Support-Aktivitäten übernehmen, um auf diese Weise schneller an sensible Kundeninformationen zu gelangen. Angreifer gehen darüber hinaus dazu über, rechtmäßige Benutzer, vor allem Schlüsselpersonen, anzusprechen, sich deren Zugriffsrechte zu erschleichen, um danach einzubrechen.

Schutz der eigenen IT-Infrastruktur

Trotz oder gerade wegen der vielen Bedrohungen von außen darf das Unternehmen den Schutz der eigenen IT-Infrastruktur keinesfalls vernachlässigen. Es muss diesen Schutz sicherstellen, indem es ihn auf den neusten Stand bringt beziehungsweise durch zusätzliche Sicherheitstechniken komplettiert. Dazu sollte das Unternehmen den Status quo der internen Sicherheitsvorkehrungen und -maßnahmen genau kennen (Assessment), um bezüglich Perimeter-Security, aber auch

Cybersecurity gezielt und angemessen darauf aufbauen zu können. Das erstrebenswerte Ziel ist dabei das technisch wie budgetär realistisch Machbare. Mit Blick auf einen angemessenen Schutz der eigenen IT-Infrastruktur heißt das:

- die internen IT-Sicherheitsschwachstellen und die daraus resultierenden möglichen Risiken analysieren,
- dazu erleuchtende Penetrationstests durchführen,
- über die klassischen IT-Security-Maßnahmen wie Firewalls oder Virenscanner sowie deren regelmäßige Updates einen Grundschutz sicherstellen,
- Intrusion Detection zur Erkennung Signatur-basierender Angriffe einsetzen und immer wieder auf den neusten Stand bringen,
- mittels Unified Threat Management (UTM) das Management der Bedrohungen zentralisieren,
- die Vergabe von Zugriffsberechtigungen zentral steuern und kontrollieren, einschließlich der Dokumentation – Auditing & Reporting – für IT-Compliance,
- sensible Datenströme verschlüsseln, ebenso alle ein- und ausgehenden E-Mails, flankiert durch leistungsfähige und ausfallsichere Anti-Spam-Software,
- mobile Endgeräte und die darauf angesiedelten IT-Ressourcen und Funktionen physisch und logisch gegen Missbrauch schützen sowie
- konsequente Durchführung von Awareness-Programmen und Mitarbeiterschulungen.

Gründliche Risikoanalyse muss sein

Was die potenziellen, neuartigen Bedrohungen aus dem Cyberspace betrifft, kommt ein Unternehmen nicht umhin, die einzelnen Bedrohungen auf die möglichen Ziele und die dort gehosteten beziehungsweise dorthin übertragenen Daten abzubilden. Nur so können die möglichen IT-Risiken und geschäftlichen Folgen analysiert und bewertet werden.

Um die Risiken im Einzelnen abwägen zu können, müssen die Entscheider wissen, in welchem Kontext die eigene IT-Infrastruktur mit den Innen- und Außenverbindungen zu den extern gehosteten oder extern bereitgestellten Daten steht. Dieses Wissen um die einzelnen Risiken und potenziellen Folgen ist außerdem die Voraussetzung dafür, um später die Beobachtung und Behebung der Risiken je nach Dringlichkeit priorisieren zu können.

Nicht mehr Sicherheit als realistisch machbar

Zudem verschafft diese Analyse Klarheit darüber, welche Risiken toleriert werden können oder sollten, beispielsweise weil die Investitionen und Aufwendungen zu ihrer Minimierung den Zugewinn an Sicherheit übersteigen würden. So ist Cybersecurity ohnehin nur annähernd realisierbar. Wird ein Großteil der Cyber-Attacken aufgedeckt und geblockt, ist viel gewonnen, gleichbedeutend mit einem erheblichen Zugewinn an Sicherheit. Dadurch sind die IT-Ressourcen, Daten und Geschäftsabläufe, vielleicht sogar das Überleben des Unternehmens im Markt, besser geschützt.

SICHERHEIT IM CYBERSPACE HERZUSTELLEN, ERFORDERT NEUE STRATEGIEN, DIE AUF EINEM SOLIDEN GRUNDSCHUTZ AUFBAUEN MÜSSEN.

AUSWAHL DER SICHERHEITSWERKZEUGE

Der Markt stellt mittlerweile eine Fülle an Tools, Schwachstellen und Exploits zur Verfügung, die zum Aufspüren von Cyber-Angriffen und potenziellen Angriffszielen herangezogen werden können. Hinzu kommen zahlreiche Cybersecurity-Techniken, die teils auf dem Grundschutz der eigenen IT-Infrastruktur aufbauen. Beispiele dafür sind:

- Perimeter & Endpoint Security
- Identity and Access Management
- Mobile Device Security
- Intrusion Detection / Prevention Monitoring
- Advanced Persistent Threat Defense
- Security Event Correlation / Analytics
- Vulnerability Testing / Vulnerability Management
- Penetration Testing
- Security Intelligence
- Verschlüsselungslösungen
- Secure E-Mail Solutions

Die Kunst besteht darin, für den eigenen Einsatz Notwendiges von nicht Notwendigem zu unterscheiden. Dabei sind auch die Ausrichtung, funktionale Abdeckungsbreite, Herkunft, Anschaffungskosten, Betriebs- und Weiterentwicklungskosten sowie mögliche funktionale Überschneidungen zwischen den unterschiedlichen Werkzeugen ins Kalkül zu ziehen.

Klare Regeln beim Einsatz externer Partner

Zuviel zu investieren ist schon deshalb nicht sinnvoll, weil die Angreifer mit ihren durch hohen Forschungseinsatz und viel Aufwand vorangetriebenen Entwicklungen den Verteidigern immer einen Schritt voraus zu sein scheinen. Unternehmen müssen mit einem Restbedrohungspotenzial leben. Externe Cloud-Betriebsmodelle schränken zusätzlich den Schutz vor Cyber-Attacken ein. Das liegt daran, dass Unternehmen in diesem Fall auch die Hoheit für die ausgelagerten IT-Teile und Daten abtreten, also bei sicherheitsrelevanten Vorfällen nicht direkt steuernd und abwehrend eingreifen können. Dennoch steht bei der Integration externer Betriebsmodelle das Unternehmen auch für die Absicherung der extern gespeicherten und verarbeiteten Geschäfts- und Kundendaten in der Verantwortung. Umso dringlicher ist es, für solche Konstellationen tragfähige Incident-/Response-Strukturen zu etablieren, klare Informationsübergabeschnittstellen zu bestimmen und für beide Seiten verbindlich festzuhalten, wer in welchem Ereignisfall welche Aufgaben übernehmen und Aktionen durchführen muss.

Beim Umsetzen einer Cybersecurity-Initiative sollten technische Werkzeuge und organisatorische Maßnahmen am Anfang stehen, die „Quick Wins“ eröffnen. Das sind Werkzeuge und Maßnahmen, die schnell implementiert werden können. Nicht zu vergessen sind flankierende Awareness-Programme zur Sensibilisierung der Mitarbeiter – ein Mix aus internen Schulungen sowie Marketing- und Aufklärungs-Aktionen. Sie sind dringend erforderlich, um im Unternehmen das notwendige Sicherheitsbewusstsein solide aufzubauen, damit Sicherheitstechniken und Menschen bestmöglich zusammenspielen.

Carsten Triebel ist Senior Consultant beim Beratungsunternehmen BridgingIT