NEUN ERFOLGSFAKTOREN FÜR EINE ERHÖHTE INFORMATIONSSICHERHEIT

Laut einer im Juni 2014 veröffentlichten Studie des Center of Strategic and International Studies verliert Deutschland jährlich 1,6 Prozent seines Bruttoinlandsprodukts durch Cyberkriminalität. Wir zeigen, wie sich Organisationen besser schützen können.

| von FLORIAN STAHL

Laut einer im Juni 2014 veröffentlichten Studie[1] des Center of Strategic and International Studies verliert Deutschland jährlich 1,6 Prozent seines Bruttoinlandsprodukts durch Cyberkriminalität. Das entsprach im Jahr 2013 in etwa 58 Milliarden Euro. Unter den 31 in der Studie untersuchten Ländern hat Deutschland damit weltweit den prozentual höchsten Schaden, gefolgt von den Niederlanden mit 1,5 Prozent und den Vereinigten Staaten mit 0,64 Prozent. Obwohl spätestens seit den Enthüllungen von Edward Snowden die Themen Datensicherheit und Cyberspionage in aller Munde sind, gibt es erhebliche Defizite bei der Wirksamkeit von Informationssicherheit in der Praxis. Zwar orientieren sich mittlerweile viele Unternehmen und Behörden an Standards wie der ISO/IEC 27001 und im öffentlichen Bereich vor allem den IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Aber dies allein reicht nicht aus, um Angreifer oder sogar Geheimdienste von vertraulichen Daten deutscher Unternehmen, Behörden oder Bürger erfolgreich fernzuhalten.

1 Center of Strategic and International Studies: Net Losses: Estimating the Global Cost of Cybercrime, URL: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf, Stand: Juni 2014

Informationssicherheit ist mehr als nur eine Frage der richtigen Technologie. Wichtig ist eine ganzheitliche Sicht auf das Thema, und zwar unter Berücksichtigung aller beteiligten Personen, erforderlichen Prozesse, Technologien und eines adäquaten Managements. So haben beispielsweise viele Unternehmen Firewalls und Antivirensoftware im Einsatz, um sich vor externen Angriffen zu schützen – der Faktor Mensch allerdings wird viel zu selten bedacht. Die Mehrzahl der Sicherheitsvorfälle wird nämlich – laut einer aktuellen Studie der Unternehmensberatung PwC[2] – durch die eigenen Mitarbeiter verursacht: einerseits, indem sie sich z. B. durch Weitergabe sensibler Daten an die Konkurrenz persönlich bereichern, andererseits, indem sie durch unvorsichtiges Handeln, durch Fehler oder Schwächen bei der Anwendung Einfallstore für Angreifer öffnen.

Systematisch berücksichtigt und abgearbeitet, erhöhen die folgenden neun Hinweise die Informationssicherheit in Ihrer Behörde:

DIE BEDROHUNG NICHT UNTERSCHÄTZEN

Viele Behörden- und Abteilungsleiter sind sich des Risikos durch Cyberangriffe oder Wirtschaftsspionage nicht bewusst und unterschätzen den daraus resultierenden Schaden für ihre Organisation oder langfristig sogar für ein ganzes Land. Die durch IT-Sicherheitsvorfälle verursachten Schäden haben in den letzten Jahren rapide zugenommen. Die Situation wird durch zunehmende Globalisierung und IT-Einsatz in allen Bereichen sehr komplex, die Risiken für den Laien kaum mehr überschaubar.

Weit verbreitet ist auch der Irrglaube, dass die Daten der eigenen Behörde oder des eigenen Unternehmens „sowieso nicht interessant sind". Aber Angreifer nehmen immer öfter auch mittlere und kleine Organisationen ins Visier. Diese haben häufig noch weniger in die Absicherung ihrer Systeme investiert, halten aber gleichzeitig wertvolle Daten und Informationen vor oder ermöglichen durch ihre Beziehungen zu Dienstleistern den Zugriff auf deren Daten. Informationssicherheit sollte daher immer mit geschulten Fachleuten umgesetzt werden und nicht von Mitarbeitern, die sich vermeintlich gut mit dem Thema auskennen.

SICHERHEITSVORFÄLLE AUFDECKEN

Möglicherweise gab es in jeder Behörde bereits Sicherheitsvorfälle, die nicht entdeckt wurden. Denn bei Datendiebstahl werden – anders als beim herkömmlichen Diebstahl von Waren – die Daten nicht entwendet, sondern lediglich kopiert. Ohne Erhebung und gezielte Auswertung von Log-Daten fallen unerlaubte Zugriffe oder Datenmanipulationen von intern oder extern oftmals gar nicht auf. Um verdächtige Aktivitäten aufzudecken, benötigt man zum Beispiel ein SIEM-System (Security Information and Event Management). Damit werden sicherheitsrelevante Log-Daten gezielt miteinander verknüpft und bei bestimmten Ereignissen, beispielsweise mehr als zehn erfolglosen Login-Versuchen von einer ausländischen IP-Adresse, wird ein Alarm ausgelöst beziehungsweise diese IP-Adresse automatisch geblockt.

NEUE BEDROHUNGEN ERNST NEHMEN, ALTE NICHT VERNACHLÄSSIGEN

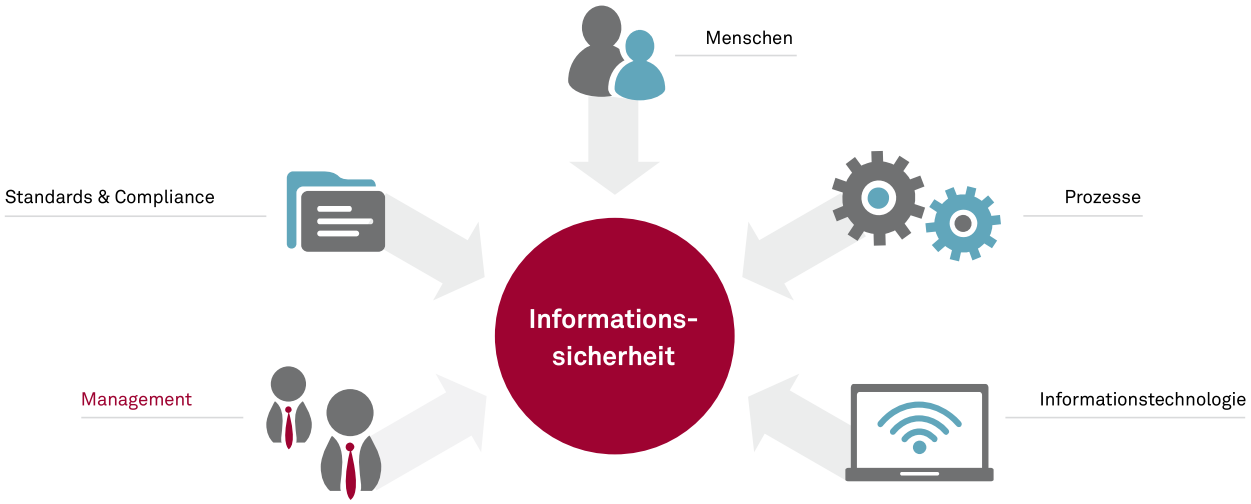
Neue Entwicklungen, wie der Einsatz von Smartphones oder mobilen Apps im Behörden- oder Unternehmensumfeld, bergen neue Risiken, die adressiert werden sollten. Mobile Endgeräte gehen leichter verloren oder werden gestohlen. Die ständige Verbindung in öffentliche und potenziell unsichere Netzwerke erlaubt neue Angriffe. Dennoch gilt es nicht nur diese „Trend-Themen" abzusichern, sondern durch einen ganzheitlichen Ansatz alle Risiken zu berücksichtigen. Schwachstellen in Web-Anwendungen sind beispielsweise bereits seit vielen Jahren ein großes Einfallstor für Angreifer, weil viele Organisationen keine durchgängigen Prozesse zur Absicherung und zum regelmäßigen Einspielen von Sicherheits-Updates (Patch-Management) etabliert haben.

Daher sollten alle Informationen und fachlichen Prozesse (Assets) systematisch erfasst werden, um alle damit verbundenen Systeme und Applikationen in zentrale Prozesse wie das Patch-Management einbinden und somit angemessen absichern zu können. Gibt es keine komplette Übersicht der vorhandenen Assets, entsteht häufig eine Systemlandschaft mit sehr unterschiedlichen Sicherheitsniveaus. Und Angreifer werden das schwächste Glied in der Kette mit Sicherheit finden.

SICHERHEIT VON BEGINN AN BERÜCKSICHTIGEN

Bei der Entwicklung neuer Lösungen sollte das Thema Sicherheit von Beginn an berücksichtigt und in die zu entwickelnde Anwendung konzeptioniert werden. Erfolgt dies erst in späteren Entwicklungsphasen, können Sicherheitslücken zwar teilweise noch behoben oder durch Firewalls oder Intrusion-Detection-/Prevention-Systeme (IDS/IPS) geschlossen werden, aber meist nur zu erhöhten Kosten. Zudem kann eine unsichere Systemarchitektur im Nachhinein in der Regel nicht mehr oder nur sehr

2 PwC: Global State of Information Security Study 2015, URL: http://www.pwc.de/gsiss2015



Einflussfaktoren für Informationssicherheit

aufwendig vollumfänglich angepasst und abgesichert werden. Sicherheit muss daher bereits während der Anforderungsanalyse großgeschrieben werden.

INFORMATIONSSICHERHEIT ZUR CHEFSACHE MACHEN

Da es um Risiken geht, die eine Bedrohung für die gesamte Organisation darstellen, sollte die Verantwortung für Informationssicherheit direkt bei der Behördenleitung (und nicht „nur" in der IT-Abteilung) liegen. Sinnvoll ist die Berufung eines Chief Security Officers (CSO), der sich auf höchster Managementebene ausschließlich mit dem Thema Sicherheit befasst. Erforderliche Maßnahmen umfassen nicht nur technische Themen, sondern auch Prozesse und Personal, die von ganz oben in die Organisation eingesteuert werden müssen. Zudem sollte der Wert der Daten (Schutzbedarf) nicht durch die IT, sondern durch die einzelnen Fachabteilungen (Datenverantwortliche) festgelegt werden. Nur sie können beurteilen, welcher Schaden durch eine Manipulation oder einen Diebstahl „ihrer" Daten verursacht würde.

AWARENESS-TRAINING FÜR ALLE DURCHFÜHREN

Informationssicherheit geht jeden an, der im Arbeitsalltag mit sensiblen Daten zu tun hat, und betrifft demzufolge (fast) alle Mitarbeiter einer Behörde. Daher sollten auch alle zum Thema Informationssicherheit sensibilisiert werden, zum Beispiel in einem Awareness-Training, in dem sie den korrekten und sicheren Umgang mit Daten lernen. Denn nicht selten werden Sicherheitsvorfälle durch die eigenen Mitarbeiter verursacht – sei es, weil ihnen die Risiken nicht bewusst sind und Daten leichtsinnigerweise über externe Cloud-Dienste wie Dropbox oder per unverschlüsselter E-Mail ausgetauscht werden oder vertrauliche Papiere im normalen Müll landen. Auch wenn häufig keine Absicht dahintersteckt, kann der Schaden immens sein. Die Studie „Cost of Data Breach 2014" des Ponemon-Instituts[3] bezifferte den durchschnittlichen Schaden einer Datenpanne in deutschen Unternehmen mit 3,4 Millionen Euro.

Vorgaben durch zielgruppengerechte Sicherheitsrichtlinien und Schutzprozesse müssen von allen Mitarbeitern konsequent gelebt werden.

TECHNISCHE LÖSUNGEN IMPLEMENTIEREN

Menschen machen Fehler. Daher ist es schwer, unbeabsichtigten Datenabfluss komplett zu verhindern. Dennoch sollte er auf ein Minimum reduziert werden. Technische Lösungen helfen, diese Fehlhandlungen zu erkennen und zu unterbinden. So könnte eine Data-Leakage-Prevention(DLP)-Lösung jeglichen Datenverkehr untersuchen, der das Unternehmen oder die Behörde verlässt. Besondere Begriffe oder Zahlenformate wie Konto- oder Kreditkartendaten oder intern eingestufte

3 Ponemon Institute: 2014 Cost of Data Breach Study (Germany), URL: http://public.dhe.ibm.com/common/ssi/ecm/en/sel03019usen/SEL03019USEN.PDF, Stand: Mai 2014

Informationen werden durch ein frei konfigurierbares Regelwerk automatisch erkannt. Folglich können sie geblockt werden, wenn sie zum Beispiel per unverschlüsselter E-Mail nach extern versendet werden sollen. Der Benutzer bekommt dabei einen Hinweis, dass sein Handeln gegen Sicherheitsrichtlinien verstößt. Beim Einsatz derartiger Lösungen werden häufig Datenschutz-Bedenken geäußert. Dient die Auswertung der Daten jedoch ausschließlich der Verbesserung der Sicherheit und nicht der Mitarbeiterüberwachung, trägt eine DLP-Lösung zur Minimierung von Geschäftsrisiken und letztlich zur Erhaltung von Arbeitsplätzen bei und sollte daher auch vom Betriebsrat unterstützt werden. Zudem müssen Verstöße gegen Sicherheitsregeln nicht auf eine Person bezogen abgespeichert werden; es genügt, sie aggregiert vorzuhalten.

Auch Passwortregelungen sollten, wo immer möglich, technisch erzwungen werden – denn Anwender halten sich erfahrungsgemäß nicht immer konsequent an rein organisatorische Vorgaben.

„KRONJUWELEN" IDENTIFIZIEREN

Eine Klassifizierung von Daten in Kategorien wie (streng) vertraulich, intern und öffentlich ist die Voraussetzung, um für jede Klasse angemessene und differenzierte Schutzmaßnahmen zu ergreifen.

Organisationen sollten sich primär um die Absicherung ihrer wichtigsten Informationen kümmern. Diese „Kronjuwelen" machen in etwa fünf bis zehn Prozent der Daten einer Organisation aus und würden bei Offenlegung, Manipulation oder Nichtverfügbarkeit signifikanten finanziellen oder Reputationsschaden bedeuten. Derartige Daten müssen identifiziert und durch Maßnahmen wie starke Authentisierung und Verschlüsselung besonders gut geschützt werden.

EXTERNE DIENSTLEISTUNGEN & PRODUKTE HINTERFRAGEN

Es gibt kaum mehr Unternehmen oder Behörden, die keine externen IT-Dienstleister oder Softwarelösungen einsetzen. Vor allem bei Anbietern oder Lösungen aus den USA oder aus China muss davon ausgegangen werden, dass Daten von Geheimdiensten mitgelesen werden. Und zwar nicht nur zur viel zitierten Terrorbekämpfung, sondern auch, um der heimischen Wirtschaft einen nachhaltigen Wettbewerbsvorteil zu verschaffen. Chinesische Router-Hersteller, amerikanische Suchmaschinenanbieter und soziale Netzwerke, aber auch Mobilfunkanbieter stellen nach aktuellem Kenntnisstand – freiwillig oder unfreiwillig – ihren Regierungen und Geheimdiensten zum Beispiel über eingebaute Backdoors (versteckte Schnittstellen zum Auslesen von Informationen) umfangreiche Daten zur Verfügung. Für deutsche Behörden und Unternehmen ist es häufig schwer, Anbieter aus diesen Ländern komplett zu vermeiden. Dennoch sollte man im Sinne der Informationssicherheit und des Datenschutzes prüfen, ob der Einsatz europäischer Partner und Lösungen das Risiko eines Daten- oder Informationsdiebstahls verringert.

Gerade in diesem Punkt ist jedoch auch die Politik gefragt und sollte ihre eigenen Interessen sowie die deutscher Unternehmen und Bürger international vertreten und durch wirksame Maßnahmen schützen. Die Verabschiedung und strikte Durchsetzung moderner Datenschutz- und IT-Sicherheitsgesetze sowie optimale Rahmenbedingungen für innovative „IT made in Germany" sind wichtige Voraussetzungen, um die Informationssicherheit gespeicherter Personen- und Unternehmensdaten und damit auch den Wirtschaftsstandort Deutschland langfristig abzusichern. ●

ANSPRECHPARTNER – FLORIAN STAHL
Lead IT Consultant
IT-Security
- +49 89 96101-1134
- florian.stahl@msg-systems.com