10 plus 1 Gedanken zum Thema Datensicherheit im Unternehmen: The Good, The Bad and the Ugly 2016

Einleitung

Der Begriff Informationssicherheit bezieht sich oft auf eine globale Informationssicherheit, bei der die Zahl der möglichen schädlichen Szenarien summarisch reduziert ist oder der Aufwand zur Kompromittierung für den Betreiber in einem ungünstigen Verhältnis zum erwarteten Informationsgewinn steht. In dieser Sichtweise ist die Informationssicherheit eine ökonomische Größe, mit der zum Beispiel in Betrieben und Organisationen gerechnet werden muss. Daneben bezieht sich der Begriff auch auf die Sicherheit unter einem bestimmten Szenarium. In diesem Sinn liegt Informationssicherheit vor, wenn über einen bereits bekannten Weg kein Angriff auf das System mehr möglich ist. Man spricht von einer binären Größe, weil die Information beim Anwenden dieser speziellen Methode entweder sicher oder nicht sicher sein kann. Gääähn….soweit die Theorie – jetzt die Praxis: 10 Tipps aus dem echten Leben:

#1 Virenschutz

Der heutige Geschäftsalltag ist ohne die Nutzung des Internets und der E-Mail-Kommunikation nicht mehr vorstellbar und zeitgemäß. Doch diese Medien bringen auch entsprechende Bedrohungen mit sich. Ein aktueller und wirksamer Schutz dagegen ist wichtig und unerlässlich. Bedenken Sie hier die unterschiedlichen Wege, die Information aus und ins Unternehmen gehen können. Es ist nicht immer nur eine heruntergeladene Datei oder ein mit Schadsoftware befallener E-Mail Anhang. Heute arbeiten immer mehr Mitarbeiter mit Werkzeugen wie Instant-Messaging (z.B.: Skype), Social Media Plattformen und Datenspeichern in der Cloud (Dropbox, OneDrive, Google Drive oder ähnliches). Auch auf diesem Weg können Daten und damit auch Schadsoftware das Unternehmen erreichen.

#2 Firewall

Eine gute Firewall schützt mich ja eh, hat mein EDV Betreuer gesagt. Mag sein, bekannt ist aber auch, dass die Mehrheit der Schadsoftware über interne Arbeitsplätze in Unternehmen eingeschleust werden. Wissen Sie wofür portable Medien (USB Sticks, Kameras, Mobiltelefone) Ihrer User verwendet werden – denken Sie auch daran, dass der private USB Stick vielleicht auch in den Firmenrechnern verwendet werden könnte.

#3 Von Arbeitsplätzen, Social Engineering, Spionage und Sabotage

Jemand der Daten aus dem Unternehmen erhalten möchte (Spionage) oder einfach dem Unternehmen schaden möchte (Sabotage) findet vielleicht auch in Ihrem Unternehmen Arbeitsplätze die heutigen Regeln der IT Sicherheit nicht mehr entsprechen. Wird jeder PC Arbeitsplatz beim Verlassen desselben gesperrt und Sie die von Mitarbeitern verwendeten Kennwörter auch sicher (siehe Abschnitt Kennwörter) oder ist es einfach der Firmenname? Probieren Sie mal das: https://nakedsecurity.sophos.com/2016/01/20/these-are-the-25-worst-passwords-of-2015-did-yours-make-the-list/

Was passiert, wenn der „fingierte“ EDV Betreuer nach dem Kennwort fragt? Probieren Sie es aus!

#4 Umgang mit mobilen Geräten

Mobile Geräte sind ja grundsätzlich was Tolles. Arbeiten überall, wann und wo ich will und ich habe meine Unterlagen mit. Das sind jedoch auch die interessantesten Möglichkeiten an zu Firmendaten zu kommen. Ein Notebook oder Mobiltelefon mit Kunden-Adressen oder Firmeninternas ist schnell geklaut oder verloren und ein Windows Kennwort auszuhebeln ist heute für jedermann mit Anleitungen aus dem Internet möglich. Eine entsprechende Verschlüsselung (z.B. BitLocker) von Notebook-Festplatten erhöht hier die Sicherheit massiv. Nutzen Sie vorhandene Technologien und Hardware-Funktionen und schaffen Sie das Bewusstsein der Datenwerte auf mobilen Geräten.

Bedenken Sie auch hier, dass nicht immer nur das Allerschlechteste (Diebstahl) eine Bedrohung darstellen. Was passiert wenn Sie Ihren Notebook zum Hersteller oder Ihre EDV Partner zur Reparatur einsenden Sie einen Rechner ausscheiden und weiterverkaufen möchten. Sind dabei die Daten sicher bzw. werden Sie vor Verlassen des Unternehmens (sicher) gelöscht? Internen Papierkram verschreddern Sie ja auch. Und was passiert im (unverschüsselten) Hotspot von McDonalds oder am Flughafen? Denken Sie auch mal darüber nach.

#5 Physische Sicherheit

Die Überwachung des Zutritts zu Serverräumen zählt zu den wichtigsten Schutzmaßnahmen. Ein Zutrittskontrollsystem

vereinigt verschiedene bauliche, organisatorische und personelle Vorkehrungen wie z.B.: Welche Bereiche? Welche Personen? Was muss protokolliert werden? Stehen Ihr Server wo?

#6 Mitarbeitersensibilisierung

Ein wichtiger Aspekt in der Umsetzung von Sicherheitsrichtlinien ist die Ansprache der eigenen Mitarbeiter, die Bildung von sogenannter IT-Security-Awareness. Hier fordern Arbeitsrichter den Nachweis der erfolgten Mitarbeitersensibilisierung für den Fall eines etwaigen Verstoßes gegen die Firmenrichtlinien. Zusätzliche Bedeutung bekommt diese menschliche Seite der Informationssicherheit außerdem, da Industriespionage oder gezielte, wirtschaftlich motivierte Sabotage gegen Unternehmen nicht allein mit technischen Mitteln ausgeführt werden. Um ihren Opfern zu schaden oder Informationen zu stehlen, nutzen die Angreifer beispielsweise Social Engineering, das nur abzuwehren ist, wenn die Mitarbeiter über mögliche Tricks der Angreifer orientiert sind und gelernt haben, mit potenziellen Angriffen umzugehen. Die Mitarbeitersensibilisierung variiert typischerweise von Unternehmen zu Unternehmen von Präsenzveranstaltungen über webbasierte Seminare bis hin zu Sensibilisierungskampagnen.

#7 Kennwörter

gelten im Allgemeinen als Sicherheitsmaßnahme um unbefugten Zugriff auf IT Infrastrukturen zu steuern. Haben Sie schon mal über eine Kennwort-Richtlinie für alle Ihre User gedacht. Ein Kennwort ist nur dann sicher, wenn es eine entsprechende Komplexität (Länge, Mischung aus Buchstaben, Zahlen und Sonderzeichen) besitzt, entsprechend oft und regelmäßig geändert werden muss und nicht einfach zu erraten ist. Moderne Betriebssysteme bieten hierzu umfangreiche Möglichkeiten für jede Sicherheitsstufe. Eine weitere Erhöhung der Sicherheit kann durch sogenannten Multi-Faktor-Authentifizierung erreicht werden. Die Anmeldung erfolgt in diesem Falle mit mehreren Informationen – etwas das ich weiss und etwas das ich besitze (z.B.: eine Kombination aus Benutzername, Kennwort, Pincode, Token und/oder Smartcard). Viel hilft Viel!

#8 Zugriffsrechte

Betriebsfremde Personen wie z.B. Mitarbeiter von IT-Dienstleistern können leicht Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar.

Externe Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, müssen schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.

Aber auch für interne Mitarbeiter sollte eine entsprechende Schulung zur Sensibilisierung der Datenverarbeitung zwingend notwendig sein. Ein IT Administrator der ungeschränkten Zugriff aus E-Mail Postfächer aller Mitarbeiter hat und das nutzt, verstösst gegen das Telekommunikationgeheimnis STGB §119 und ist mit Freiheitsstrafe bis zu sechs Monaten zu bestrafen – fragen Sie mal Ihren Admin danach.

#9 Protokollierung

Auf Protokollierung und dementsprechende Verwendung und Verwahrung der Protkolle sollte geachtet werden. Frei nach dem Motto: Was passiert, wenn etwas passiert? Als Beispiele sind folgende Links angeführt:

- www.internet4jurists.at/literatur/datensicherheit.pdf
- https://www.wko.at/Content.Node/Service/Wirtschaftsrecht-und-Gewerberecht/Verwaltungs--und-Verfassungsrecht/Datenschutz/Datensicherheit_-_Was_verlangt_das_DSG_2000_.html

Wer darf was aufzeichnen, wer darf das Einsehen und wofür verwenden? Haben Sie darüber schon nachgedacht?

#10 Spielregeln und Usage Policies

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ausgeprägtes Sicherheitsbewusstsein besitzen und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen. Schulung und Sensibilisierung für Fragen der IT-Sicherheit sind daher unbedingt notwendig.

Es empfiehlt sich, Regelungen zu folgenden Bereichen zu treffen, die in Form einer Verpflichtungserklärung von allen Mitarbeitern zu unterzeichnen sind: PC Benutzungs-Richtlinien, Benutzung für Internet und E-Mail und das Datengeheimnis (§15 DSG).

und der Bonus: #11 Datensicherung

ist für jeden Betrieb mittlerweile selbstverständlich. Oft verlässt man sich allzu gerne auf die Kompetenz des EDV Fachmannns für die Auswahl und den Zyklus der zu sichernden Daten. Klassifizieren Sie Ihre Daten und überlegen Sie mit welchen Daten Sie in einem Notfall und in welchem Intervall und Zeitraum Sie Ihre Daten benötigen und prüfen Sie in regelmäßigen Abständen ein Wiederherstellungsszenario.

Bei der Aufbewahrung der Backup-Datenträger ist aus zwei Gründen besondere Sorgfalt angebracht: Die Entwendung eines Sicherungsmediums würde einem Angreifer den

einfachen Zugriff auf die wichtigsten Unternehmensdaten ermöglichen. Und im Katastrophenfall, etwa nach der Zerstörung der IT-Systeme durch einen Brand, sind die Sicherungen die einzige Chance, den elektronisch gespeicherten Datenbestand zu retten.

Weitere Informationen:

z.B. unter
www.bmi.gv.at/cms/BK/praevention.../IT_Sicherheitshandbuch.pdf

Viel Spass beim Nachdenken und Umsetzen.

www.egos.co.at/securityseminare

Kontakt

EGOS! The Education Company
Entwicklungsgesellschaft für Organisation und Schulung GmbH
Eduard Bodem Gasse 1/III
6020 Innsbruck

www.egos.co.at

facebook.com/egos.education