„WannaCry“: Existenzbedrohende Millionenstrafen bei Datendiebstahl!

Praxistipps zum Schutz Ihrer Kundendaten als Vorbereitung auf die Datenschutz-Grundverordnung

Am 24. Mai 2016 ist die europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft getreten. Allerdings mit einer Übergangsfrist von 2 Jahren, damit sich die Länder und vor allem die Unternehmen darauf vorbereiten können. D.h. die extrem strenge Datenschutz-Grundverordnung wird spätestens ab 25. Mai 2018 angewendet werden müssen.
Damit kommt es zu massiven Änderungen. Zwei davon: Die Strafen werden drastisch verschärft und die Meldepflichten an die Datenschutzbehörden fallen weg. Die neuen Regelungen gelten für alle Unternehmen, die Finanz- und Versicherungsbranche werden aber wohl besonders streng behandelt werden, weil wir sehr viele sensible Daten (Finanz, Gesundheit etc.) der Kundinnen und Kunden haben. Große Unternehmen werden sich „einiges“ einfallen lassen müssen, Klein- und Mittelbetriebe sollten zwar auch ihre Prozesse näher beleuchten, könnten aber mit der Befolgung einiger Praxistipps die größten Gefahrenquellen für „Datenverlust“ beseitigen.

Genau darum geht es heute in diesem Beitrag. Um weitere Aufgaben, wie etwa Datenschutz-Abwägungen, Datenschutzverantwortliche, Mitarbeiter-Schulung etc. wird es in einem der nächsten Beiträge gehen.

Zu Beginn zu den zwei gravierenden Änderungen:

a) Exorbitante Strafhöhe:
Bisher waren die Strafen mit max. EUR 10.000 sehr bescheiden und haben wohl kaum ein Großunternehmen „erschreckt“. Nun jedoch drohen EUR 5 Mio. oder 4 % des jährlichen Konzernumsatzes. Das wird sogar Konzerne wie Google, Facebook und Co „zum Nachdenken bewegen“. Und das dürfte auch der Hintergedanke dieser unglaublichen Strafandrohung sein.

b) Meldepflichten weg, Beweislastumkehr:
Bisher musste man seine Datenprozesse an die Datenschutzbehörde melden. Das fällt weg. Was als Vorteil gesehen werden kann, bringt aber eine Beweislastumkehr mit sich. Zwar muss man jetzt nichts mehr melden, erhält aber dadurch auch keine Genehmigung der Behörde im Vorfeld. Wenn etwas passiert, ist man dafür „alleine verantwortlich“ und muss beweisen, dass man alles „Denkbare“ getan hat, um den Datendiebstahl zu vermeiden.

Das kann mich doch nicht betreffen! Oder doch?

Vor wenigen Wochen sprach jeder vom „WannaCry“-Hackerangriff. Ein Wurm verbreitete sich blitzschnell im Netz, infizierte die Infrastruktur von vielen Unternehmen und Institutionen (Krankenhäuser in Großbritannien, Deutsche Bahn, spanische Telefonica, Autokonzerne Renault und Nissan, Ölkonzern PetroChina, russisches Innen- und Katastrophenschutzministerium etc.). Bei den Betroffenen wurden die Dateien auf dem Computer verschlüsselt und für die Freigabe wurde Lösegeld verlangt.
EDV-Experten (wie z.B. Mag. Georg Markus Kainz) und die Polizei raten übrigens, nicht zu bezahlen, weil man keine Sicherheit hat, dass man tatsächlich das Passwort zur Freigabe erhält und auch nicht weiß, ob die Daten – trotz Bezahlens – nicht trotzdem anderweitig verwendet, verkauft werden.

Nun zu den Praxistipps:

a) Tagesaktuelle Datensicherung
Ist man bereits in der oben beschriebenen Situation und die Dateien sind verschlüsselt, dann hilft nur noch, den PC neu aufzusetzen und die Daten von einer Sicherung wieder einzuspielen. Dazu muss man aber eine möglichst aktuelle Sicherung haben.

Zum Thema Datensicherung haben wir bereits einen Praxistipp verfasst. Hier zum Nachlesen.

b) Wie kann ich vermeiden, überhaupt in diese Notlage zu gelangen?

b1) Software installieren und aktuell halten, d.h. automatische Updates erlauben
Firewall, Anti-Viren-Software und Co sollten in jedem Unternehmen vorhanden sein.
Leider werden diese Programme, aber auch die verwendeten Betriebssysteme (Windows) und Office- und sonstige Programme, nicht aktuell gehalten.

Software besteht aus Millionen von Programmzeilen. Hacker suchen und nutzen Fehler in diesen Programmzeilen und gelangen auf diesem Wege in Ihr System.
Daher aktivieren Sie überall die „Automatischen Updates". Dann werden Änderungen – sobald Fehler erkannt wurden – automatisch auf Ihrem Computer eingespielt.

b2) Ausfallsicherheit & Verschlüsselung
Um im Falle eines Falles „rasch umschalten" zu können, empfiehlt es sich, die Daten möglichst aktuell auf einer zweiten Festplatte oder einem USB-Stick „zu spiegeln", also doppelt zu schreiben. Dann kann man die Daten von dieser Sicherung auf einem anderen PC oder dem neu aufgesetzten PC rasch wieder herstellen.

Wichtig ist, dass man externe Festplatten, USB-Sticks aber z.B. auch Laptops verschlüsselt, damit ein Hacker nicht auf die Daten zugreifen kann. Dazu gibt es zahlreiche Programme. In Windows ist standardmäßig das einfach zu bedienende Bitlocker-Programm vorhanden. Nutzen Sie es. Hier wählen Sie ein Passwort aus und verschlüsseln damit. Ohne dieses Passwort einzugeben, kann niemand auf die Daten zugreifen.

b3) Sicheres Passwort wählen ist eigentlich ganz einfach:
Immer wieder kann man lesen, dass die am häufigsten verwendeten Passwörter „Passwort", „12345" oder die Namen der Kinder, Haustiere etc. seien.
Das ist zwar verständlich, weil man sich heute zahlreiche Zugangsdaten merken muss, trotzdem grob fahrlässig.

EDV-Experten schlagen vor, dass das Passwort 8 - 20 Zeichen beinhalten und aus Buchstaben, Zahlen und Sonderzeichen bestehen soll. Auch Groß- und Kleinschreibung ist hilfreich. Aber wie kann man sich „AmEsadSusw." merken???

Dafür empfehlen die Experten, sich einen markanten Satz zu suchen und dann die Anfangsbuchstaben der einzelnen Wörter zu verwenden. So empfahl z.B. Tele 2:
Aus dem Satz „Meine Fußballmannschaft hat nur noch 1 Stunde Zeit um ein Tor zu schießen, damit sie die Meisterschaft gewinnen kann!" das Passwort: „MFhnn1SZueTzs,dsdMgk!".

Möchte man nicht auf jeder Seite das gleiche Passwort verwenden, dann empfiehlt sich eine jeweilige Ergänzung dieses Satzes um den Einsatzort und Jahreszahl (etwa Telekom2017).
Da damit wieder zahlreiche Passwörter entstehen, kann das Nutzen eines Passwort-Safes, wie etwa kostenloser Keypass-Software, hilfreich sein. Man muss sich dann nur noch ein Master-Passwort zum Einstieg merken. Die einzelnen Passwörter speichert dann dieser Tresor. Die Software können Sie kostenlos hier herunterladen.

Wenn Sie Firefox als Internetbrowser verwenden, können Sie dort ebenfalls die Verwendung eines Master-Passworts einstellen. Einfach rechts oben auf Einstellungen und dann auf Sicherheit klicken und einen Haken bei „Master-Passwort verwenden" setzen. Nutzen Sie diese Option nicht, sind die Angaben zu Kontonamen und Passwörter nicht geschützt und können von Hackern leicht ausgelesen werden.
Probieren Sie es selbst aus. Klicken Sie im Firefox auf Einstellungen – Sicherheit und „Gespeicherte Zugangsdaten" und Sie werden überrascht sein, wie lange die Liste der Kennwörter ist. Ein Hacker hätte nun die Info, wo Sie aktiv sind und wie Ihre Zugangsdaten lauten. Unter der Annahme, dass viele Menschen die gleichen Zugangsnamen und Passwörter bei vielen Konten verwenden, kann man sich das Bedrohungspotential dann besser vorstellen.

b4) Hinterfragen Sie nützliche aber potentiell gefährliche Tools
Viele von uns nutzen Smartphones oder Tools wie Dropbox oder Cloud-Systeme. Das ist überaus praktisch aber potentiell gefährlich. Warum? Es handelt sich zumeist um amerikanische Anbieter. In den USA ist der Datenschutz für ausländische Kundinnen und Kunden (also uns) fast nicht existent. Bei Bedrohungen sind die amerikanischen Firmen sogar zur Zusammenarbeit mit Nachrichtendiensten verpflichtet. Von den bekannt gewordenen E-Mail-Mitlese-Aktivitäten von NSA und Co ganz zu schweigen.
Wenn Sie nun etwa ein iPhone oder iPad nutzen, dann haben Sie wahrscheinlich auch die Apple-Cloud zur Speicherung aktiviert. Und schon sind Ihre Daten – und womöglich auch Ihre Kundendaten – in einer amerikanischen Umgebung gespeichert und damit nicht mehr wirklich geschützt.
Datenschützer empfehlen daher die Verwendung eines europäischen Cloud-Anbieters oder die Cloud ebenso zu verschlüsseln wie ein externes Laufwerk (siehe Tipp b2).

Dropbox und ähnliche Dienste versprechen die einfache Zusammenarbeit mehrerer Personen auf mehreren Arbeitsplätzen. Man kann damit einzelne Dokumente, ganze Datenordner oder sogar den ganzen PC für Dritte freigeben. Das bedeutet aber in der Praxis, dass Sie damit einem Dritten Lese- und Schreibzugriff auf Ihre Daten erlauben. Das ist wohl mit Datenschutz nicht vereinbar!

b5) Automatisches Ausführen von VB-Scripts bzw. Plugins verhindern
Da sich Viren und bösartige Schadsoftware (Malware, Trojaner etc.) oftmals durch Exe-Dateien verbreiten oder mit Hilfe von Plugins die Internet-Browser befallen und damit den kompletten PC verseuchen, sollte man dies verhindern. Ihr EDV-Berater stellt Ihnen das entsprechend ein.

Oftmals kommen solche gefährlichen Dateien als Anhänge zu E-Mails, daher sollten Sie auch den nächsten Tipp beachten.

Im nächsten BAV-Newsletter setzen wir diesen Beitrag fort und berichten über die Gefahrenquelle „E-Mail-Programm" und geben Tipps, wie man gefälschte E-Mail-Absender bzw. Web-Adressen erkennt". Auch „Phishing Mails" und die „Anlaufstelle Internet-Ombudsmann" werden praxisnah behandelt werden.

Quellen: Mag. Günter Wagner, B2B-Projekte; Mag. Georg Markus Kainz, Quintessenz; Internet Ombudsmann; Watchlist Internet; chip.de; pcwelt.de; Newsletter Tele 2; Outook.com; medianet.at, trend.at