Cyber Crime und wie Sie sich schützen können

Wolfgang Sidler, Inhaber SIDLER Information Security GmbH und Partner der SASERA AG, Master of Advanced Studies in Information Security, Certified ISO 27001 Lead Auditor und Mitautor des «IT-Sicherheitshandbuches für die Praxis» www.sihb.ch

Die schnelle Digitalisierung und Mobilität verursacht neue Gefahren und exponiert sensible Unternehmensdaten und stellt für die Unternehmen eine grosse Herausforderung dar. Auch das Verhalten der Benutzer hat sich massiv und schnell verändert. Geschäftsdaten überall, zur jeder Zeit und auf jedem Gerät.

Die Bedrohungslage hat sich insoweit geändert, dass die Mittel dazu moderner werden, die Mitarbeitenden immer vernetzter sind und dass ein zu geringes oder gar kein Sicherheitsbewusstsein vorhanden ist. Die grosse Herausforderung ist die Balance zwischen «Sicherheit und Bedienbarkeit».

Nach RUAG Vorfall war das Statement von Bundesrat Guy Parmelin «KMU sind sich der Gefahr zu wenig bewusst». Fremde Staaten können E-Mails, Faxe, Telefone durch Satelliten abhören und Wanzen installieren oder können durch IT-Angriffe via Trojaner in Ihr IT-System eindringen und dort meistens unbemerkt Informationen sammeln und weiterleiten (z. B. unbemerktes Weiterleiten aller E-Mails).

Problematisch ist auch die schnell zunehmende Vernetzung zwischen den industriellen Kontrollsystemen wie Produktionsmaschinen und den Desktop-Arbeitsplätzen sowie den mobilen Geräten der Ingenieure oder Wartungspersonal, welche wiederum oft einen Internetzugang haben.

So entsteht eine Schatten-IT und Mitarbeitende verwenden z. B. Dropbox umso sensible Geschäftsdaten zur eigenen Bequemlichkeit hochzuladen um diese dann später zu Hause oder unterwegs auf private Notebooks oder Tablets zu kopieren.

Mobile Kommunikation ist zum wichtigen Ansatzpunkt geworden, um an sensitive geschäftliche und persönliche Informationen zu gelangen. Denn an keiner anderen Stelle kann man so schnell derart viele persönliche und wichtige Informationen abgreifen. Was lange ausschliesslich eine Domäne von Geheimdiensten war, ist durch technischen Fortschritt und dem Preisverfall beim Equipment zu einem Standard-Werkzeug für Wirtschaftsspionage und Computer-Kriminalität geworden. Was mit dem Smartphone gerade passiert ist für den Benutzer nicht erkenntlich. Und keine IT Abteilung ist vor Ort und kann die Sicherheit der Verbindung überprüfen. Dazu kann ein Smartphone heute gleichzeitig im Mobilfunknetz und über WLAN im firmeneigenen Netzwerk eingeloggt sein. Über diese «Funkbrücke» werden abgeschottet geglaubte Bereiche in einem Unternehmen plötzlich von aussen mit schnellen Mobilfunk-Zugängen erreichbar. Ohne dass der Benutzer es merkt, kann über das SS7 Protokoll über den Basenet Protokoll-Stack z. B. das Mikrophon eingeschaltet werden.

Am 21. Dezember 2016 hat der Bundesrat die Vernehmlassung zur Totalrevision des Bundesgesetzes über den Datenschutz eröffnet. Bis am 4. April 2017 läuft die Vernehmlassung mit dem Ziel, dass das neue Schweizer Datenschutzgesetz im Mai 2018 in Kraft treten soll.

Unternehmen ist dringend zu empfehlen, sich bereits jetzt auf die neue Gesetzgebung einzustellen und die notwendigen Vorbereitungsarbeiten zur Sicherstellung der künftigen Datenschutzkonformität an die Hand zu nehmen. Dazu gehören z. B. die Analyse der Datenbearbeitungsprozesse und der damit verbundenen Risiken, der bestehenden internen Richtlinien und Weisungen sowie der Verträge mit Dritten, an welche Daten weitergegeben werden oder die Daten im Auftrag bearbeiten, und gestützt darauf die Überprüfung des Anpassungsbedarfs und die Vorbereitung der für dessen Umsetzung erforderlichen Massnahmen. Die bisherige maximale Busse bei Verletzung von datenschutzrechtlichen Pflichten betrug lediglich CHF 10'000.–. Neu wird die maximale Busse auf CHF 500'000.– erhöht durch die Unterlassung der Information der Betroffenen, von angemessenen Massnahmen zur Gewährleistung der Datensicherheit, der Datenschutz-Folgeabschätzung oder der Dokumentation der Datenbearbeitung. Zudem müssen Datenschutz-Vorfälle neu dem eidg. Datenschützer gemeldet werden.

Der Hype um die Clouds verschärft das Thema. Der Nutzer weiss in der public Cloud (z. B. Amazon oder Microsoft) nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider seine Daten speichert. In den entsprechenden Service Level Agree-

ments (SLA) kann zum Beispiel der folgende Passus stehen «Unter bestimmten Umständen kann (Name des Providers) Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen». Für ein rechtlich abgesichertes Cloud-Szenario sind dedizierte Anforderungen an den Cloud Provider sowie wasserdichte Verträge ein Muss. Es ist nicht die Frage ob etwas passieren wird, sondern wann. Welche Gefahren bedrohen unsere innovativen CH-Unternehmen?

Wie können Sie sich schützen?

- Zeigen Sie Management-Attention in Bezug auf die Informationssicherheit und Datenschutz.
- Sensibilisieren Sie alle Mitarbeitenden in Bezug auf die Informationssicherheit (z. B. Umgang mit Smartphones, BYOD, Phishing, Clear Desk Policy, etc.)
- Beginnen Sie ein Informationssicherheits-Managementsystem (ISMS) aufzubauen (Notfall- und Krisenmanagement-Konzept, ein Risiko-Management-Konzept, eine Cloud-Strategie, eine Mobile-Device Strategie, ein übergreifendes Berechtigungskonzept für den Zugriff auf vertrauliche Daten, etc.), welches Sie später gemäss ISO 27001 zertifizieren lassen können.
- Erstellen Sie eine IT-Nutzungsweisung z.B. Umgang mit E-Mail und Internet, Akten-Vernichtung, Umgang mit USB-Sticks, etc.
- Führen Sie Security-Audits und Schwachstellen-Scans durch, um mögliche Schwachstellen (technisch wie auch organisatorischer Natur) im Unternehmen zu finden und zu beheben.
- Verschlüsseln Sie Ihr Daten bevor Sie diese in einer Public-Cloud (z.B. Microsoft Office 365, Salesforce) speichern.
- Verschlüsseln Sie die Festplatte Ihres Notebooks z.B. mit BitLocker von Windows 10 und einer Pre-boot Authentifizierung.
- Verschlüsseln Sie vertrauliche Dokumente, welche Sie via E-Mail versenden. Nur mit einer angemessenen Verschlüsselung können Sie die Vertraulichkeit wahren.
- Behandeln Sie geschäftliche Themen und Informationen in der Öffentlichkeit vertraulich während einer Bahn- oder Flugreise oder im Restaurant. Lassen Sie andere nicht mithören und lassen Sie sich nicht aushorchen.
- Schliessen Sie vertrauliche Unterlagen weg. Verlassen Sie Ihren Arbeitsplatz jeweils aufgeräumt (Clear Desk). Werfen Sie keine Datenträger (CDs) und Dokumente mit sensiblem Inhalt ungeschreddert in den Papierkorb. Wenn Sie Ihren Arbeitsplatz auch nur für kurze Zeit verlassen, aktivieren Sie Ihren Bildschirmschoner.
- Installieren Sie keine unbekannte Software. Vorsicht bei Freeware-Software. Stellen Sie sicher, dass die Quelle vertrauenswürdig ist. Halten Sie Ihren Virenschutz und Ihre Programme inkl. Betriebssystem auf dem aktuellsten Stand.
- Führen Sie mit Hilfe eines Sicherheitsspezialisten eine Risiko-Analyse in Ihrem Unternehmen durch. Dabei geht es darum, die Unternehmenswerte zu identifizieren, damit die Risiken und Gefahren explizit richtig eingeschätzt werden können. Ermitteln Sie die möglichen Szenarien mit den entsprechenden Gegenmassnahmen.

Fazit

Die Bedrohungen und der damit verbundene Datenabfluss ist eine Realität. Durch die wachsende Komplexität und Vernetzung der IT-Systeme und die Globalisierung ergeben sich neue Herausforderungen an den Schutz der Daten und Informationen. Schützen Sie Ihr Firmen-Know-how mit Ihren Möglichkeiten und lassen Sie sich wenn nötig von einem Sicherheitsspezialisten beraten. Befolgen Sie die hier beschrieben Tipps und Empfehlungen, die dazu beitragen werden, Ihr Firmen-Know-how angemessen zu schützen. *Wolfgang Sidler*

Sidler Information Security GmbH
Holzhäusernstrasse 5a, 6331 Hünenberg
Telefon 41 781 57 72
wolfgang.sidler@sidler-security.ch
www.sidler-security.ch

Am 4. Mai 2017 findet das erste «Lucerne Law & IT Summit 2017» unter dem Patronat der UNI Luzern mit hochkarätigen Speakers statt.
www.unilu.ch/weiterbildung/rf/weiterbildung-recht/lucerne-law-it-summit-lits
www.workingwell.ch