Sicherheitsrisiko Mitarbeiter
Unterschätzte Gefahr durch „Hired Hackers“

Passwortdiebstahl, Hackerangriffe, Malware – Geht es um Sicherheit und Datenschutz in Unternehmen, scheinen die größten Gefahren stets von Dritten auszugehen. Dabei wird jedoch häufig die Tatsache übersehen, dass erhebliche Sicherheitsrisiken auch aufgrund interner Faktoren drohen. Während Unternehmen regelmäßig hohe Summen in den Schutz ihrer IT-Infrastruktur investieren, um sich vor Angriffen von außen abzusichern, lassen viele das Problem der inneren Sicherheit völlig außer Acht.

Über die mögliche Anwendung schadhafter Software hinaus wird vor allem das Fehlverhalten von Mitarbeitern zu einem immer größeren Problem. Denn im Zeitalter des mobilen Internets nutzen Angestellte Smartphones, Tablets und Co. häufig nicht nur privat, sondern auch geschäftlich. Ob es nun die eigenen Endgeräte sind oder firmeneigene Hardware, oftmals werden unternehmensinterne Sicherheitsrichtlinien unbewusst, aber auch bewusst umgangen. Laut einer aktuellen Studie des Marktforschungsunternehmens OnePoll wissen rund 47 Prozent der Mitarbeiter in deutschen Unternehmen nicht, ob ihr Arbeitgeber Sicherheitsbestimmungen bezüglich der Nutzung von mobilen Geräten vorschreibt bzw. kennen den Inhalt vorhandener Richtlinien nicht. Gut 29 Prozent verwenden ihre privaten Geräte ebenso für Arbeitszwecke, ohne zu wissen, ob sie überhaupt dazu befugt sind.[1]

Gefahrenquelle Mobile Security

Was in Unternehmen häufig ignoriert wird, sind mögliche Konsequenzen, die sich aus dem unbefugten Einsatz mobiler Geräte für die geschäftliche IT-Infrastruktur bzw. die Datensicherheit ergeben können. Ein Beispiel ist etwa das unüberlegte und unautorisierte Installieren von Apps auf firmeneigenen Endgeräten. Oftmals ist Nutzern nicht bekannt, auf welche Funktionen das fragliche Programm zugreifen kann. So rufen einige Apps ohne Wissen des Anwenders dessen Kontakte, gespeicherte Dateien oder seinen Standort ab. Auf diese Weise wird unbemerkt Fremdzugriff auf das Firmennetzwerk ermöglicht. Ähnliche Szenarien ergeben sich für private Endgeräte, auf denen sich meistens schon eine Vielzahl heruntergeladener Apps befindet. Wer diese Geräte für geschäftliche Zwecke nutzt, kann nicht sicher sein, dass seine Daten nicht von Dritten mitgelesen werden. Dies ist aber nur eines von vielen Sicherheitsrisiken. Weitere Bedrohungen ergeben sich zudem durch die unerlaubte Nutzung von öffentlichen Cloud- und Sharing-Programmen.

Cyber-Risiken oft hausgemacht?

[1] OnePoll & Samsung Electronics, „People-Inspired Security“, 2014

Sogenannte „Hired Hackers“ werden der OnePoll-Studie zufolge immer mehr zu einem erheblichen Sicherheitsrisiko. Dabei handelt es sich um technisch versierte Mitarbeiter, die des Öfteren zum Smartphone oder Tablet greifen, um sich die Arbeit zu erleichtern. Meist kennen sie firmeninterne Sicherheitsbestimmungen und wissen diese geschickt zu umgehen. Unternehmen sollten dahingehend Maßnahmen ergreifen, um mögliche Risiken auszuschalten. Tun sie das nicht, drohen nach Inkrafttreten der neuen EU-Datenschutzverordnung zukünftig horrende Geldstrafen bei Verstößen gegen geltende Sicherheitsrichtlinien.

Alexander Krist, IT-Sicherheitsexperte der circular Informationssysteme GmbH, erklärt in diesem Zusammenhang: „Am wichtigsten ist, die Mitarbeiter im Hinblick auf einen verantwortungsvollen Umgang mit sensiblen Firmendaten zu schulen – und zwar kontinuierlich. Unternehmen müssen aufklären und ihre Angestellten mit den IT-Sicherheitsvorgaben vertraut machen.“ Das betrifft nicht nur den Umgang mit firmeneigenen Endgeräten, sondern auch die Nutzung von privaten Geräten in Verbindung mit geschäftlichen Applikationen sowie den Gebrauch von externen Speichermedien wie etwa USB-Sticks.

[Kasten]

Schutz von Unternehmen vor möglichen Sicherheitsrisiken:

1. Aufklärung der Belegschaft zu den Sicherheitsbestimmungen bezüglich der Nutzung von mobilen Endgeräten im Unternehmen
   ➔ Wer darf wann und womit auf welche Informationen zugreifen?

2. Schulung der Mitarbeiter zum richtigen und sicheren Umgang mit sensiblen Firmendaten
   ➔ Dürfen Angestellte auch mit ihren eigenen mobilen Endgeräten auf Geschäftsanwendungen zugreifen?

3. Informieren der Mitarbeiter hinsichtlich einer fehlerfreien Verwendung ihrer Passwörter
   ➔ Trennung von privaten und geschäftlichen Kennwörtern

4. Installation von Schutzsoftware
   ➔ Verhindert unbefugten Zugriff von Dritten und legt Backup vorhandener Daten an

5. Herunterladen und Installieren von vertrauenswürdigen Applikationen
   ➔ Apps, die nicht überprüft wurden, sind möglicherweise ein Risiko für mobile Endgeräte sowie sensible Geschäftsdaten

6. Regelmäßiges Update aller Applikationen
   ➔ Schützt vor möglichen Sicherheitslücken

7. Ausschalten von Ortungsdiensten auf Smartphone, IPad & Co.
   ➔ Zugriff auf die Ortungsfunktion könnte ein weiterer Angriffspunkt sein

Über circular

Gegründet 1995, hat sich die circular Informationssysteme GmbH zu einem System- und Beratungshaus im Bereich IT-Infrastruktur entwickelt. Das umfangreiche Portfolio beinhaltet Lösungen rund um die Themen IT-Sicherheit, Data Center, Netzwerke und Communications. Die Dienstleistungskette reicht von der IT-Strategieberatung über die Projektplanung und -durchführung, die Lieferung von Hard- und Software, Systemintegration und Wartung bis hin zur Schulung. Neben dem Hauptsitz in Stuttgart unterhält das Unternehmen mit 55 Beschäftigten weitere Niederlassungen in München, Frankfurt, Berlin, Leipzig und Hamburg. Die IT-Spezialisten betreuen Kunden aus den Branchen Industrie, öffentliche Verwaltung, Service Provider, Finanzen, Gesundheitswesen sowie Forschung und Lehre.