iwd

Informationen aus dem Institut der deutschen Wirtschaft Köln

Cyberkriminalität | 10.02.2017 | Lesezeit 3 Min.

So verhindert man den Datenklau

Datenklau und Social Engineering sind für die Unternehmen ein großes Geschäftsrisiko – noch vor Betriebsunterbrechungen. Dabei gibt es einfache Tricks, wie sich Mitarbeiter sicherer im Internet bewegen und damit auch ihr Unternehmen schützen können.

Naturkatastrophen, austrittswillige EU-Länder oder die Eurokrise – all das gefährdet die Geschäfte deutscher Unternehmen lange nicht so sehr wie Cyberattacken, hat das Risk Barometer der Allianz ergeben. Denn neben einfachen IT-Ausfällen kommt es vermehrt zu Hacking, Datenschutzverletzungen und Datendiebstahl. Rund zwei Drittel der Industrieunternehmen waren in den Jahren 2014 und 2015 von Cyberkriminalität betroffen. Den dadurch entstandenen Schaden beziffert der Digitalverband Bitkom auf rund 22,4 Milliarden Euro – pro Jahr. Das Spektrum der Attacken reicht von simpel bis spektakulär (Grafik):

Während den Unternehmen der Diebstahl von IT-Geräten meist noch auffällt, tun sie sich deutlich schwerer damit, E-Mails und andere elektronische Daten vor unberechtigtem Zugriff zu schützen.

Tatort Unternehmen

So viel Prozent der Unternehmen in Deutschland waren in den Jahren 2014 und 2015 von diesen kriminellen Vorfällen ...

■ ... betroffen ■ ... vermutlich betroffen

	... betroffen	... vermutlich betroffen
Diebstahl von IT- oder Telekommunikationsgeräten	32	10
Diebstahl von sensiblen Dokumenten, Bauteilen, Maschinen	20	11
Diebstahl von sensiblen elektronischen Dokumenten oder Informationen	19	16
Sabotage von Betriebsabläufen	18	15
Social Engineering	16	17
Ausspähen von elektronischer Kommunikation, z.B. E-Mails	6	23
Abhören von Besprechungen oder Telefonaten	5	12

Befragung von 504 Industrieunternehmen mit mindestens zehn Mitarbeitern im November/Dezember 2015; Social Engineering: Angriffe auf Informationssysteme mithilfe psychologischer Tricks gegenüber Mitarbeitern mit dem Ziel, ihnen interne und sensible Informationen zu entlocken

Quelle: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom)

Institut der deutschen Wirtschaft Köln

Dabei nutzen Angreifer nicht nur technische Sicherheitslücken, sondern zunehmend auch menschliche Schwächen wie Hilfsbereitschaft oder Habgier aus, um Passwörter oder komplette Datensätze abzuschöpfen. „Social Engineering“ heißt dieses Phänomen, bei dem Mitarbeiter gezielt ausgehorcht und manipuliert werden, um an vertrauliche Firmeninformationen zu gelangen.

Sechs Tipps gegen den Datenklau

Gänzlich verhindern lassen sich Cyberattacken sicher nicht. Doch es gibt einige Instrumente für Internetnutzer – sowohl beruflich als auch privat –, mit denen sie sich vor Angriffen aus dem Netz schützen können.

1. **Sicherer surfen.** Häufig wird das Internet über einen Browser genutzt. Mithilfe von Cookies, das sind kleine Computerprogramme, verfolgen viele Browser das Surfverhalten der Nutzer und verknüpfen es mit anderen Informationen. In den Einstellungen der Browser können diese Cookies gelöscht werden. Das Browser-Add-on-Programm Disconnect.me blockiert Cookies und Schnüffelprogramme. Firefox beispielsweise gehört zu den sichereren Browsern, da man ihn anpassen und nachvollziehen kann, wie er funktioniert. Im „Privaten Modus“ kann das Internet genutzt werden, ohne dass Firefox Daten über die Webseitenbesuche, Formulareinträge oder Cookies speichert.

> Angreifer nutzen zunehmend menschliche Schwächen wie Hilfsbereitschaft oder Habgier aus, um Passwörter oder Datensätze abzuschöpfen.

---

1. **Passwort-Sicherheit.** Die meisten Menschen wählen zu einfache Passwörter. Es ist wichtig, für jede Anwendung und jedes Onlinekonto unterschiedliche Passwörter zu nutzen. So sollten keine Wörter aus dem Wörterbuch verwendet werden, da es Computerprogramme gibt, die jedes einzelne Wort aus dem Wörterbuch automatisch ausprobieren, um Passwörter zu erraten. Je komplexer ein Passwort, desto größer der Schutz. Ein sicheres Passwort sollte mindestens zwölf Stellen haben. Merken kann man sich das Passwort über Eselsbrücken. „KgdFalSm1z0!“ kann etwa „Köln gewann das Finale am letzten Samstag mit 1 zu 0!“ bedeuten. Speichern lassen sich die vielen Passwörter am besten in einer verschlüsselten Datei in einem Passwort-Manager.

1. **Nachrichten verschicken.** Viele Smartphone-Messaging-Apps speichern die Texte und Kontaktdaten ihrer Nutzer. Das kann man leicht umgehen, denn es gibt

auch Messenger, die keine Daten sammeln – zum Beispiel die Whatsapp-Alternative Signal. Mit ihr kann man verschlüsselte Nachrichten schreiben und verschlüsselt telefonieren.

1. **Smartphone-Sicherheit.** Viele Smartphone-Apps greifen auf mehr Informationen zu, als sie müssten. Bei der Installation von Apps ist es verlockend, die Nutzungsbedingungen einfach zu akzeptieren, ohne sie zu prüfen. Dabei ist offensichtlich, dass zum Beispiel eine Taschenlampen-App keinen Zugriff auf das Adressbuch benötigt. Oft lassen sich in den Einstellungen die Zugriffsrechte der Apps einschränken.

1. **Sperren und Updates.** Eine Bildschirmsperre schützt Arbeitscomputer und Handy vor dem ungewollten Zugriff durch Dritte. Software-Updates sollten regelmäßig installiert werden, denn sie beheben oft Schwachstellen wie Sicherheitslücken in den Anwendungen. Das gilt auch für Browser-Updates.

1. **Erste Hilfe im Ernstfall.** Im Falle eines Hacks sollten Nutzer sofort das Passwort des betroffenen Onlinedienstes ändern und prüfen, ob das E-Mail-Postfach ebenfalls gehackt wurde. Auch das Umfeld sollte rasch informiert werden – vor allem innerhalb von Unternehmen verbreiten sich Cyberangriffe oft schnell. Häufig ist sogar externe Hilfe nötig. Das Bundesamt für Sicherheit in der Informationstechnik bietet Beratung bei Cyberangriffen, in Bayern ansässige Unternehmen und Hochschulen können sich zudem an das Cyber-Allianz-Zentrum des Bayerischen Landesamts für Verfassungsschutz wenden.

Darüber hinaus sollte nicht zu früh Entwarnung gegeben werden, denn IT-Angriffe sind in der Regel nicht auf kurze Zeit limitiert. In den Wochen und Monaten nach einer Attacke kann es immer wieder zu Nachwehen kommen.

Kernaussagen in Kürze:

- Mehr als zwei Drittel der deutschen Industrieunternehmen waren in den Jahren 2014 und 2015 Opfer von Cyberkriminalität.
- Angreifer nutzen längst nicht mehr nur technische Sicherheitslücken, sondern zunehmend auch menschliche Schwächen aus, um an firmeninterne Informationen zu gelangen.
- Den Schaden, der durch Cyberangriffe auf Industrieunternehmen entsteht, beziffert der Digitalverband Bitkom auf rund 22 Milliarden Euro im Jahr.