

Von fehlenden Sicherheitsrichtlinien, dem Faktor Mitarbeiter und dem falschen Umgang mit Passwörtern...

Herr P. ist Inhaber einer mittelständischen traditionsreichen Herrenboutique. Für seine Geschäftskorrespondenz, Statistiken, Konzepte, Kunden- und Lieferantenkartei hat Herr P. einen PC mit Internetzugang. Hierüber wickelt er auch online seine Bankgeschäfte ab, checkt regelmäßig seine eMails und nutzt das Internet zur Beschaffung und für Recherchezwecke. Aus Vereinfachungsgründen verwendet Herr P. ein und dasselbe Passwort für alle Zwecke. Damit er sich das Passwort leicht merken kann, hat er als Passwort den Vornamen seines Kindes gewählt. Benutzername ist sein eigener Nachname. Einigen der 20 Angestellten ist das Passwort des Herrn P. bekannt, weil Herr P. bei EDV-Problemen gerne die Hilfe seiner Mitarbeiter in Anspruch nimmt und dabei seine Zugangsdaten preis gibt.



Seit einem halben Jahr sind die Umsätze um knapp 15 % zurückgegangen. Einige seiner Stammkunden scheinen vermehrt bei der vor einem Jahr neueröffneten Boutique „Men“ zu kaufen, die zusätzlich zum stationären Verkauf über einen Online-Shop verfügt. Als Herr P. eines Tages ein Zeugnis für eine Mitarbeiterin schreiben will, sucht er als Vorlage das Zeugnis, welches er vor knapp 1,5 Jahren seiner ehemaligen Mitarbeiterin Frau K. ausgestellt hat, die er aufgrund von Unzuverlässigkeit und häufiges Zuspätkommen entlassen musste. Mit Erschrecken stellt er fest, dass das Zeugnis zum Positiven abgeändert wurde. Die Datei wurde zuletzt an einem Tag geändert, wo er im Urlaub war.

Was ist geschehen?

Frau K. hat sich unbefugt in den PC von Herrn P. eingeloggt, ihr Zeugnis geändert und wichtige Geschäftsdaten wie die Lieferanten- und Kundendatei sowie den Business Plan auf eine CD gebrannt und gestohlen. Ihr Lebensgefährte ist Inhaber der neueröffneten Boutique „Men“ und hat die Geschäftsdaten des Herrn P. genau analysiert und für seine Zwecke missbraucht.

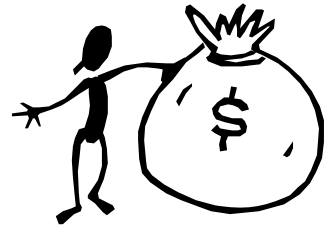


Gehe nicht zu sorglos mit Passwörtern um...

Beim Zugang zum Rechner oder auf das Internet, beim Online-Banking oder beim Checken der eMails, immer wieder wird Herr P. dazu aufgefordert, seine Berechtigung durch ein Passwort nachzuweisen. Auch die modernen Techniken (Chipkarten, biometrische Verfahren) werden in absehbarer Zeit wenig daran ändern, dass Passwörter die wichtigsten Mittel sind, den Zugang zu einem Rechner oder zu einer Anwendung zu schützen. Ein zu sorgloser Umgang mit Passwörtern (zu kurze oder erratbare Kennwörter) macht es anderen leicht, sich unbefugten Zutritt zu dem Rechner und den darin enthaltenen Daten zu verschaffen.

Wer den Schaden hat...

Herr P. vermutet, dass sich seine ehemalige Mitarbeiterin Frau K. unbefugten Zugang zu seinem PC verschafft und wichtige Geschäftsdaten gestohlen hat. Spezialisten können mit Hilfe geeigneter Werkzeuge nachweisen, dass auf dem PC Dateien kopiert worden sind. Allerdings kann Herr P. seinen Verdacht nicht beweisen. Die Boutique „Men“ ist zu einem harten Konkurrenten geworden, bietet ein ähnliches Sortiment an, aber konnte in den Bereichen, in denen die traditionsreiche Herrenboutique ihre Schwachstellen hat (nicht mehr die neuste Ladengestaltung, kaum innovative Marketingkommunikation,...), wesentliche Wettbewerbsvorteile erzielen und spricht aggressiv viele seiner Stammkunden an. Herr P. hat seine ausgezeichnete Marktstellung eingebüßt, was zu einer Verschlechterung seiner wirtschaftlichen Lage geführt hat.



■

Was tun?

Die Sicherheit der Zugangs- und Zugriffsrechteverwaltung ist entscheidend davon abhängig, dass Passwörter korrekt gebraucht werden. Dafür ist es empfehlenswert, den Umgang mit Passwörtern ganz klar zu regeln (→ schriftliche Dokumentation) und die Mitarbeiter diesbezüglich zu unterweisen.



Grundsätzlich sollten Sie folgende Punkte beachten:

- Schaffen Sie Bewusstsein, dass Passwörter geknackt werden können.
- Passwörter müssen sicher gewählt werden.
- Passwörter müssen gut merkbar sein.
- Passwörter sollten von Zeit zu Zeit gewechselt werden.
- Passwörter für verschiedene Zwecke sollten unterschiedlich sein.
- Passwörter sollten nicht auf dem Rechner gespeichert werden.

Das BSI-Grundschutzhandbuch hat dazu folgende Empfehlungen herausgegeben
(Quelle: www.bsi.de/gshb/deutsch/m/m2011.htm):

Regelung des Passwortgebrauchs

1. Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist.
2. Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.
3. Das Passwort darf nicht zu kompliziert sein, damit der Besitzer mit vertretbarem Aufwand in der Lage ist, es auswendig zu lernen.

Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?
- Wird die Passwort-Güte kontrolliert?
- Wird der Passwort-Wechsel erzwungen?
- Ist jeder Benutzer im Netz mit einem Passwort ausgestattet?

... und darüber hinaus

Im Rahmen der „organisatorischen Sicherheit“ gibt es eine Vielzahl weiterer Maßnahmen, die im Unternehmen Anwendung finden sollten, um einen Missbrauch oder Datenverlust zu vermeiden:

- Schaffen Sie Berechtigungsprofile.
- Stellen Sie Zugangskontrollen zu den Rechnern her.
- Verbieten Sie oder schränken Sie das Mitbringen fremder Datenträger ein, die Viren enthalten können.
- Verpflichten Sie die Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen.
- Schulen Sie Ihre Mitarbeiter zu IT-Sicherheitsmaßnahmen.
- Sensibilisieren Sie die Mitarbeiter für mögliche IT-Gefährdungen.

Weitere Informationen unter:

Technologietransfer im Handel
www.Technologietransfer-Handel.de

Bundesamt für Sicherheit in der Informationstechnik
<http://www.bsi.de/gshb/deutsch/m/m2011.htm>

Gefördert vom:

Technologie Transferstelle des Handels in Niedersachsen
beim Bildungszentrum des Einzelhandels Niedersachsen
Kurzer Ging 47
31832 Springe

Fon: 05041 – 788-37

Mail: thekla.krammer@bze-springe.de

Fax: 05041 – 801632 Web: www.bze-springe.de

Gefördert vom Bundesministerium für Wirtschaft und Arbeit

