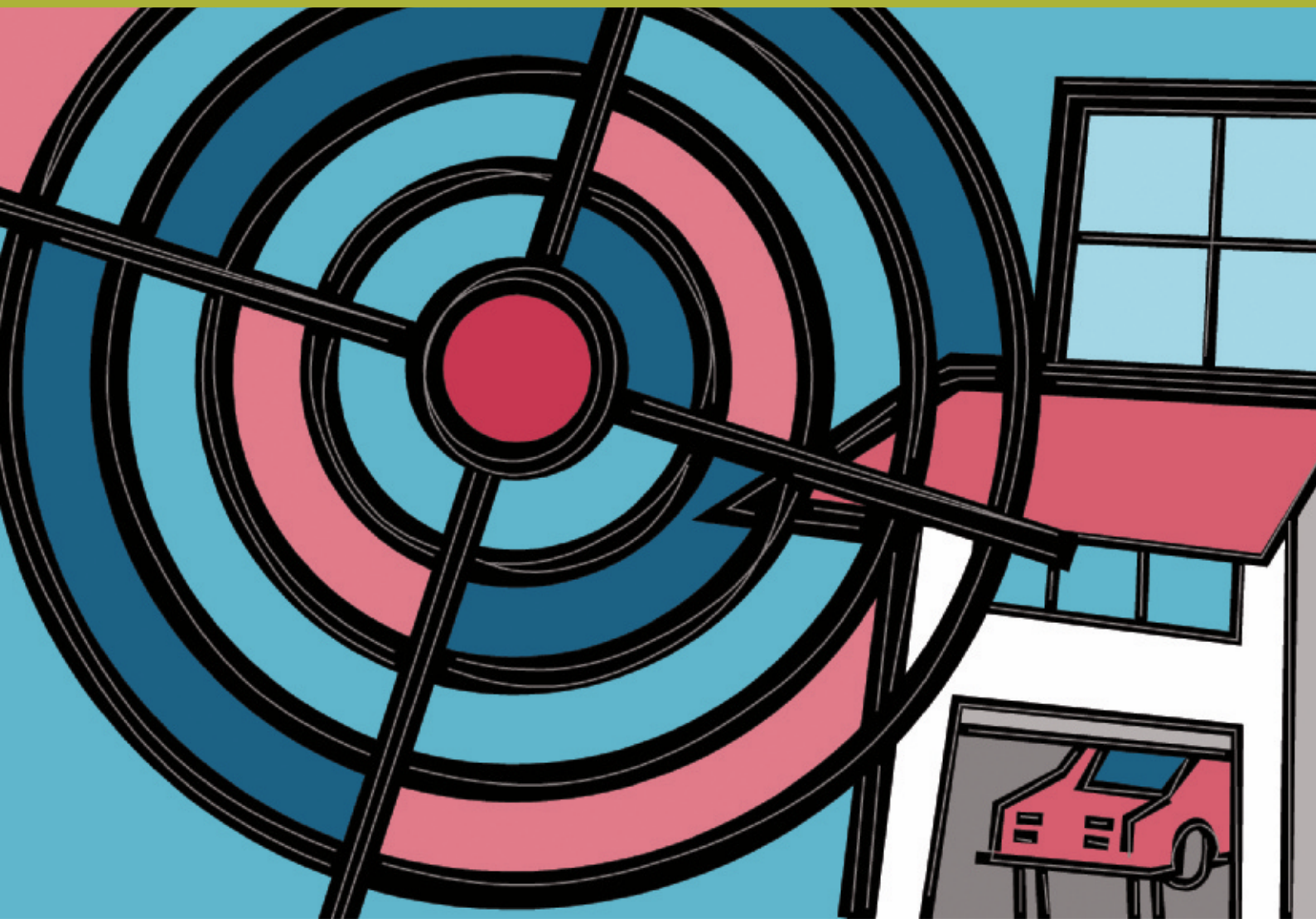

KMU im Hacker-Visier: ICT-Angriffe abwehren

Informatik und Telekommunikation jedes Unternehmens sind hohen Risiken ausgesetzt. Während Grossunternehmen sich der Gefahren bewusst sind, setzen KMU meist andere Prioritäten. Dabei wären auch für sie ICT-Strategien und entsprechende Sicherheitskonzepte enorm wichtig. VON ARMIN BAUMANN

Risiken in einem Unternehmen sind mehrschichtig, und die Unternehmer sind oft überfordert und ohne Hilfsmittel. Wenn eine Produktionsmaschine ausfällt, lässt sich der entstandene Schaden relativ gut beziffern. Springt ein Kunde ab, kann das entstehende Problem ebenfalls gut eingeschätzt werden. Weitere Risikoquellen stellen Sachschäden (Feuer, Wasser, Strom), Krankheit oder Unfälle von Mitarbeitern, Rechts- und Versicherungsfälle, Umweltbelastung, Finanzen, Planungsfehler, Transportschäden oder Lieferengpässe dar. Ein ganz besonders hohes Risikopotential bergen überdies Informatik und Telekommunikation (ICT). Einerseits kann ein Ausfall der ICT die komplette Firma oder zumindest Teile des Unternehmens lahmlegen. Andererseits können wertvolle Informationen aus dem Unternehmen gestohlen oder manipuliert werden.

Die ICT bildet für viele Unternehmen einen unverzichtbaren Lebensnerv. Denn über sie wird mit den Kontaktgruppen (Kun-

Hier lesen Sie ...

- weshalb auch KMU eine IT-Security-Strategie benötigen
- wie eine solche Strategie geplant und umgesetzt wird
- weshalb der Schutzgrad nicht höher als nötig gewählt werden sollte

den, Mitarbeiter, Lieferanten, Partner) kommuniziert und die stetig steigende Datenflut bewältigt. Dennoch haben – wie eine Studie der ABA Management zeigt – 85 Prozent der kleinen und mittleren Unternehmen keine ICT-Strategie. Dies ist nicht verwunderlich, da rund zwei Drittel der KMU die ICT als Kostenfaktor und nicht als unternehmerisches Differenzierungspotential betrachten. Es bedeutet allerdings auch, dass die ICT-Risiken in den KMU als zu gering erachtet werden.

«Die Informatik und die Kommunikation sind der Lebensnerv vieler Firmen. Daher müssen sie geschützt werden.»

Armin Baumann ist Initiant der Plattform KMU SWISS AG und Geschäftsführer der ABA Management GmbH. Er war Dozent für Marketing an der Privaten Hochschule Wirtschaft (PHW) und ist Autor des Buches «Marketinggrundlagen für KMU – einfach und verständlich».

Zwei wesentliche Punkte bilden im ICT-Umfeld je ein Risiko: Wissen und Image! Dass ein ICT-Ausfall Kosten verursacht ist ebenso klar wie die Tatsache, dass der Ausfall unmittelbare Auswirkungen auf das operative Geschäft hat. Entstehende Imageschäden sind von nicht abschätzbarer Ausprägung, denn sie haben schnell Auswirkungen auf das Unternehmen und können nur mit grossem Aufwand wieder neutralisiert werden. Eine alte Weisheit sagt: «Wissen ist Macht.» Heute ist nicht der Stärkere, sondern der Schnellere erfolgreich. Oder anders ausgedrückt: Wer das Wissen hat, steht den Anderen vor der Sonne! Früher entstanden Angriffe und Spionage aus dem Jargon des Militärs. Heute wird nicht mehr nur Krieg auf dem Schlachtfeld geführt, sondern in allen Bereichen der Wirtschaft.

Das Unternehmenswissen wird dabei hauptsächlich in zwei Risikogruppen «gespeichert»: Mitarbeiter und Informatik. Die Konkurrenz benötigt Informationen, um sich gegenüber einem Mitbewerber einen Wettbewerbsvorteil verschaffen zu können. Auch die Medien leben von Informationen. Und je aktueller diese sind, umso besser verkauft sich die Botschaft. Selbst Nachrichtendienste interessieren sich für Wirtschaftsinformationen aus anderen Ländern, um die eigene Nation besser positionieren zu können. Der schnellste Weg, um an zusätzliches Wissen zu kommen, sind veröffentlichte Informationen im Internet oder anderen Medien wie TV, Radio oder Print. Der zweite, etwas anspruchsvollere Weg, ist das Abgreifen der Informationen von Mitarbeitern. Indem man mit diesem kommuniziert – am Telefon, via E-Mail oder persönlich. Der dritte und aufwendigste Weg ist das Knacken der Informatik durch professionelle Hacker.

Mitarbeiter, als schwächstes Glied der Informationsquelle, können durch laufende Aufklärung, Sensibilisierung und definierte Richtlinien dazu bewegt werden, dass sie nicht unabsichtlich Informationen an unerwünschte Personen weitergeben.

Hackerangriffe auf eine KMU-Informatik werden in der Regel über eine Firewall, wahlweise auf den Web-/Mail-Server respektive File-/Datenbank-Server lanciert. Dabei werden die Hacker immer raffinierter. Um Spam-Filter zu umgehen, verzichten sie etwa darauf, ihre Botschaften mit bösartigen Codes zu versehen. Stattdessen integrieren sie Links, die zu Web-Seiten mit grossem Schadenpotenzial führen. Klickt der Empfänger diese Links an, ist das Problem vorprogrammiert. So können unerlaubte Personen auf nicht mehr geschützte Informationen zugreifen oder das System lahmlegen. Das Unangenehme dabei ist, dass betroffene Unternehmen erst reagieren können, wenn es bereits zu spät ist. Zwar gibt es keine hundertprozentige Sicherheit – aber ein hohes Mass an Sicherheit ist dennoch zu erreichen. Dazu muss man aber Bedrohungen rund um die Uhr erkennen und darauf reagieren können. Die Unterstützung durch erfahrene Spezialisten ist in diesem Bereich sicher sinnvoll. Für eine erste Einschätzung sollen mögliche, entstandene Schäden eingestuft und darauf basierend ein entsprechendes Budget zur Umsetzung abgeleitet werden.

Risikomanagement in fünf Schritten

1. **Aufnahme des «Ist»-Zustandes**
   Identifizieren Sie Risiken, bewerten Sie diese und schätzen Sie mögliche entstehende Schäden ein. Daraus leiten Sie das entsprechende Umsetzungsbudget ab.
2. **Definierung des «Soll»-Zustandes**
   Bestimmen Sie Ihre Ziele: Was muss bis wann erreicht werden?
3. **Festlegung der ICT-Security-Strategie**
   Legen Sie Massnahmen fest, wie der Veränderungsprozess vom Ist- auf den Soll-Zustand erreicht werden kann. Dann planen Sie die Umsetzung (eventuell als Phasenmodell).
4. **Umsetzung der Massnahmen**
   Setzen Sie die festgelegten Massnahmen um und implementieren Sie den zuvor definierten Schutz.
5. **Controlling der Schutzmassnahmen**
   Überwachen Sie regelmässig alle implementierten Schutzmassnahmen, und passen Sie diese regelmässig an die jeweils aktuellen Anforderungen an.

Bei der Erarbeitung des Risikomanagements gilt dasselbe wie bei der ICT-Strategie: Damit die Umsetzung vom Gesamtunternehmen getragen wird, müssen bei der Erarbeitung alle involvierten Menschen mit einbezogen werden. Getreu dem Motto: «Was alle angeht, können nur alle lösen!» Wichtig ist, den Sicherheits- respektive Schutzgrad nur so hoch zu wählen, dass die Sicherheitskultur von allen Betroffenen auch gelebt werden kann und nicht als Hindernis dem Unternehmenserfolg im Wege steht. ■