



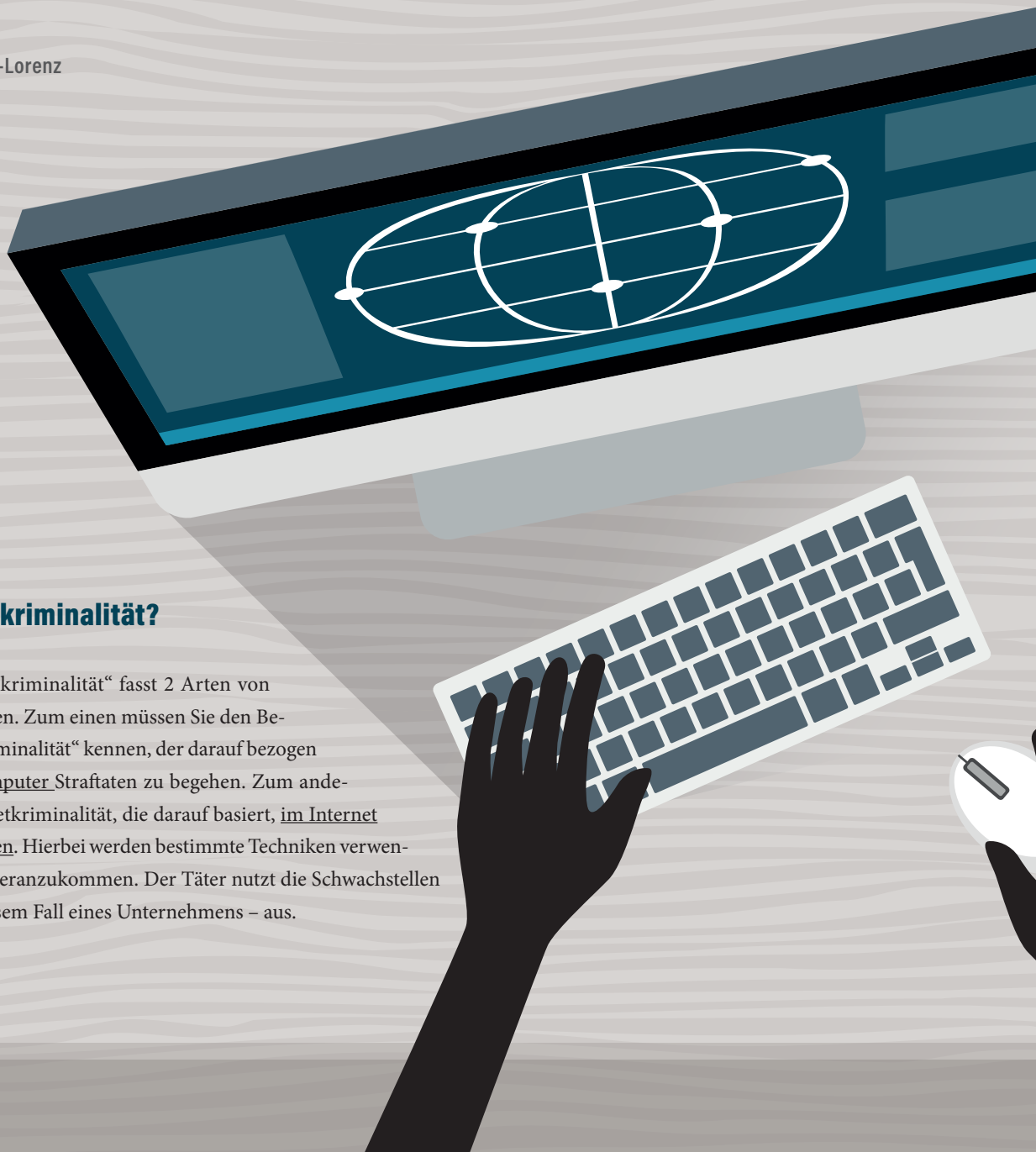
So schützen Sie Ihre Daten vor Cyberkriminalität

Je digitaler die Welt und die gesamten Prozesse innerhalb Ihres Unternehmens werden, umso mehr Angriffsfläche bieten sie Kriminellen. Vor allem Unternehmen stehen im Visier der Hacker und die Straftaten sowie Datendiebstähle nehmen immer mehr zu. Im Interesse der Kriminellen stehen Dokumente, Schnittstellen und Nachweise im Bereich der Exportkontrolle. Unsere Übersicht zeigt Ihnen, welche Daten Sie besonders schützen und welche Maßnahmen Sie ergreifen sollten – und zwar schon, bevor etwas passiert.

Von Julianna Straib-Lorenz

Was ist Cyberkriminalität?

Der Begriff „Cyberkriminalität“ fasst 2 Arten von Straftaten zusammen. Zum einen müssen Sie den Begriff „Computerkriminalität“ kennen, der darauf bezogen ist, mit einem Computer Straftaten zu begehen. Zum anderen existiert Internetkriminalität, die darauf basiert, im Internet Straftaten zu begehen. Hierbei werden bestimmte Techniken verwendet, um an Daten heranzukommen. Der Täter nutzt die Schwachstellen des Opfers – in diesem Fall eines Unternehmens – aus.



Welche Schwachstellen gibt es in einem Unternehmen?

Ein Unternehmen kann viele Schwachstellen haben. Die wichtigsten schauen wir uns hier an:



1. **E-Mails:** Denn durch das Klicken auf einen Link in der E-Mail oder das unbedachte Öffnen angehängter Dateien durch die Mitarbeiter starten die Straftäter ihre Hackerangriffe auf Unternehmen.



2. **Ransom-Mails:** Mit Ransom-Mails möchten Straftäter durch verschlüsselte Daten und sensible Inhalte etwas hervorrufen. Meistens sind diese Daten so sensibel, dass die Empfänger mit den Inhalten erpresst werden.



3. **Internetzugang und Internetseiten:** Ein offenes Internet ist immer sehr gefährlich, denn es gibt viele Seiten, die Viren oder Trojaner enthalten. Hier ist Ihre IT-Abteilung gefragt, denn durch eine Firewall können viele Fehler vermieden werden.



4. **CD-ROMs und USB-Sticks:** Mittlerweile ist es jetzt schon gang und gäbe, dass man in Unternehmen keine fremden Sticks oder CD-ROMs einlesen darf. Denn hier ist die Gefahr sehr groß, dass durch fremde Daten Viren und/oder Trojaner in das System der Firma eingespeist werden.

Diese Daten gilt es zu schützen

Im Bereich der Exportkontrolle bzw. für eine Außenwirtschaftsprüfung benötigen Sie neben dem Ausfuhrbegleitdokument auch interne Unterlagen wie Rechnungen, Stücklisten, Datenschutz-Blätter, Kundenangaben, Firmenprofile und Vertragsunterlagen. Des Weiteren sind Endverbleibserklärungen und entsprechend dazu auch die Ausfuhr genehmigungen wichtig und schützenswert.

Ergreifen Sie folgende Maßnahmen

Wenn Sie noch eine Papierablage haben, haben Sie hier die Sicherheit, dass Sie wichtige Dokumente vor digitalem Datenskandal schützen, sofern Sie diese auch ablegen. Haben Sie eine digitale Ablage, sollten Sie vorsorglich folgende Maßnahmen ergreifen:

1. Machen Sie das Thema zur Chefsache und beziehen Sie die obere Führungsebene mit ein.
2. Erstellen Sie einen Notfallplan, was im Fall eines Hackerangriffs zu tun ist.
3. Klären Sie im Vorfeld die Ansprechpersonen und Verantwortlichkeiten.
4. Klären Sie im Vorfeld mit Ihrem Dienstleister oder Ihrer IT-Abteilung, wie digitale Dokumente gesichert werden. Hierbei geht es um Backups oder gesicherte Kopien aller Daten.
5. Schalten Sie sofort die Polizei (<https://bit.ly/33Gp5Ho>) ein, wenn etwas passiert, und melden Sie Ihren Vorfall innerhalb von 72 Stunden der Datenschutzaufsichtsbehörde Ihres Bundeslandes (<https://bit.ly/33Gp5Ho>), dem Bundesamt für Sicherheit in der Informationstechnik (<https://bit.ly/3uIebwO>).

