
Foto: tostphoto – stock.adobe.com

# Geschulte Mitarbeiter wichtig für Sicherheit

## Erklärungen zur IT-Sicherheitslinie der KZBV – Teil 5

Ein allzu großes Vertrauen in Technik kann zuweilen schädlich sein. Das zeigt sich auch im Bereich der IT-Sicherheit: Technik allein bietet keinen ausreichenden Schutz. Der Mensch wird jedoch häufig bei der Entwicklung von Sicherheitskonzepten vollständig ausgeblendet. Dabei sind gut geschulte Mitarbeiter die effektivste Maßnahme gegen Cyberkriminalität.

In den Beiträgen dieser Reihe standen bislang IT-Notfallkonzepte, der Umgang mit datenschutzrelevanten Vorgängen und die Nutzung von Cloud-Lösungen im Mittelpunkt. Sie nahmen Bezug zur IT-Sicherheitsrichtlinie der KZBV und beschrieben Forderungen der Richtlinie und deren praktische Umsetzung.

Diese Initiative der KZBV ist sehr zu begrüßen. Sucht man allerdings im entsprechenden Dokument nach den Begriffen „Sensibilisierung“ oder „Schulung“, so erhält man keine Treffer. Sucht man nach dem Begriff „Mitarbeiter“, so erhält man lediglich Treffer im Zusammenhang mit Richtlinien, die von Mitarbeitern eingehalten werden sollen.

Foto: Hans Schenkel

Dr. Thomas H. Lenhard ist ein international anerkannter Experte für Informationstechnologie und Datenschutz. Er greift auf seinen umfangreichen Erfahrungsschatz aus drei Jahrzehnten Datenschutz und Datensicherheit zurück und ist u.a. als Datenschutzbeauftragter für die DGI e.V. umfassend tätig.

Hier greift die IT-Sicherheitsrichtlinie nach Meinung des Autors deutlich zu kurz. Dieser Beitrag wird diese Einschätzung begründen und beschreibt, was Sie in Ihrer Praxis, im MVZ, in der Klinik oder Institution unbedingt beachten sollten, selbst wenn Sie durch die IT-Sicherheitsrichtlinie nicht direkt dazu verpflichtet sind.

Vor einiger Zeit ging eine Eilmeldung durchs Netz, dass Cyberkriminelle eine neue, sehr perfide Masche einsetzten, um Ransomware zu verbreiten. Ransomware sind Schadprogramme, die beispielsweise Daten verschlüsseln. Kriminelle setzen sie ein, um Nutzer und Firmen zu erpressen.

Diese Warnmeldung ging auch bei dem externen Datenschutzbeauftragten eines Unternehmens morgens kurz nach 8 Uhr ein. Da eine Mitarbeiterin der Firma bereits durch ihren unbedarften Umgang mit IT-Anlagen in der Vergangenheit aufgefallen war, kontaktierte der Datenschutzbeauftragte zusätzlich zur Aussendung per Rundmail den Geschäftsführer des Unternehmens noch vor 9 Uhr am selben Tag und wies auf die Gefährdung hin. Die Erwi-

derung des Geschäftsführers: „Zu spät!“ Dank eines vorausschauenden und kompetenten IT-Verantwortlichen konnte der Schaden jedoch ohne einen Abfluss von Daten schnell behoben werden. Das Beispiel zeigt gleichwohl, dass Mitarbeiterinnen und Mitarbeiter ganz wesentlich dazu beitragen können, ob Daten und IT-Anlagen sicher oder in höchstem Maße gefährdet sind.

**So gelangt Ransomware auf IT-Systeme.** Sehr häufig verwenden Kriminelle E-Mails mit getarnten Links. Werden diese angeklickt, wird die Schadsoftware auf den Rechner des Opfers geladen. Auch Loader und Skripte, die als E-Mail-Anhang versendet werden, kommen zum Einsatz. Beide Verfahren laden weitere Schadsoftware auf einen Rechner, sobald sie gestartet werden.

Auch über externe Datenträger kann Schadsoftware auf Rechner gelangen. Weitere Quellen von Schadsoftware sind per E-Mail übermittelte Informationen, Downloads aus unsicheren Quellen, unsichere Webseiten, vermeintliche Updates oder angeblich notwendige Einstellungsänderungen, Fake-Meldungen („Ihr Rechner ist infiziert“) oder Anrufe wegen angeblicher Sicherheitsprobleme.

**Häufig verwenden Kriminelle E-Mails mit getarnten Links. Werden diese angeklickt, wird die Schadsoftware auf den Rechner des Opfers geladen.**

**Hacker spielen kaum noch eine Rolle.** Dem ein oder anderen Leser wird hier bereits aufgefallen sein, dass von dem „bösen Hacker“, der irgendwo im Halbdunkel eines hochtechnisierten Kellers sitzt und Sicherheitssysteme überwindet, bei der Aufzählung keine Rede ist. Das liegt daran, dass das aktive Hacking beim Verteilen von Schadprogrammen kaum mehr eine Rolle spielt.

Vielmehr ersinnen Kriminelle ständig neue Methoden, wie sie Nutzer dazu bringen, einen Virus oder ein Schadprogramm selbst zu installieren. Oft wird dabei mit Angst gearbeitet. Mitarbeiter werden von Kriminellen so manipuliert, dass sie den Befall des Systems erst möglich machen. Technische Absicherungen werden dann mitunter ausgehebelt – wenn auch in guter Absicht und in Unkenntnis der tatsächlichen Gegebenheiten.

**Sensibilisierung ist wichtig.** Viele Vorfälle wären vermeidbar, wenn Mitarbeiter für die Gefahren hinreichend sensibilisiert wären. Schließt etwa ein Mitarbeiter einen privaten, mit einem Virus verseuchten USB-Stick in der Praxis an einen Rechner an, wird zunächst dieser Rechner und danach das gesamte Praxisnetz infiziert. Ein solches Verhalten zeugt von einem fehlenden Bewusstsein für diese Gefahren. Das Anbringen von Zetteln mit Passwörtern oder Accountdaten an Monitoren ist ebenfalls ein deutliches Indiz für schwerwiegende Sicherheitsprobleme.

Auch wenn in den meisten Fällen ein unbedarfter Umgang mit IT-Anlagen oder eine fehlende Sensibilisierung die Ursachen sind, verzeichnen Datenschützer und IT-Sicherheitsexperten auch zuweilen Zwischenfälle, denen Vorsatz oder zumindest bedingter Vorsatz zugrunde liegen.

**Ein klassischer Fall.** Ein Beispiel dafür aus einer Klinik: Die Infektion des IT-Netzes dieser Klinik hatte einige Tage zuvor einen finanziellen Schaden im sechsstelligen Bereich verursacht. Im Rahmen der Schadensbehebung wurde das bestehende Antivirensystem vollständig durch das System eines anderen Anbieters ersetzt. Zusätzlich wurde ein System installiert, das die Nutzung von externen Datenträgern überwacht und in der zentralen IT-Abteilung sofort einen Alarm auslöst, wenn ein nicht autorisierter Datenträger verwendet werden sollte. In diesem Zusammenhang wurden alle Mitarbeitenden darauf aufmerksam gemacht, dass externe Datenträger verboten sind.

Wenige Tage später löste das System Alarm aus. Ein Mitarbeiter hatte versucht, einen mit Viren verseuchten USB-Stick an einen Rechner der Klinik anzuschließen. Vom IT-Verantwortlichen zur Rede gestellt, gab sich der Mitarbeiter nicht etwa reumütig, sondern erklärte, dass es ihm „sch… egal“ sei, ob er einen Virus einschleppen würde. Die „Kulissenschieber aus der IT-Abteilung“ hätten das Virus „dann gefälligst wieder zu beseitigen“.

**Das Anbringen von Zetteln mit Passwörtern oder Accountdaten an Monitoren ist ein deutliches Indiz für schwerwiegende Sicherheitsprobleme.**

Von derartigen Mitarbeitern geht in aller Regel ein extrem hohes Gefährdungspotenzial aus. Bedenkt man, dass ein solches Fehlverhalten den Fortbestand einer Institution gefährden oder Patienten schädigen könnte, liegt auf der Hand, dass ein Verantwortlicher hier unbedingt und unverzüglich einschreiten muss.

Schließlich gibt es auch Mitarbeiter, die zwar hervorragende Arbeit leisten, aber nicht sonderlich IT-affin sind. Diese sind in aller Regel sehr vorsichtig. Sie sind aber, gerade aufgrund ihrer niedrigen Affinität, auch besonders anfällig für Machenschaften Krimineller.

Auf dieser Basis lassen sich drei Szenarien beschreiben, die zu einer erhöhten Gefährdungslage im Zusammenhang mit der IT-Sicherheit führen können:

- Die Mitarbeiter sind für Belange der IT-Sicherheit nicht ausreichend sensibilisiert und geschult.
- Einzelne Mitarbeiter sind wenig IT-affin und daher anfällig dafür, von Kriminellen manipuliert und als „Werkzeug“ eingesetzt zu werden.
- Einzelnen Mitarbeitern ist es egal, ob durch ihr Handeln der Institution ein Schaden entsteht.

Bei dieser Aufzählung fehlt die vorsätzliche Sabotage durch Mitarbeiter, da dies mit den nachfolgend beschriebenen probaten Mitteln häufig nicht zu verhindern ist

und weitergehende organisatorische und technische Maßnahmen erfordert.

**Risiko: menschliches Verhalten.** Wie lassen sich Gefahren für die IT-Sicherheit minimieren, die im Zusammenhang mit menschlichem Verhalten stehen? Soweit ein Datenschutzbeauftragter für die Institution bestellt wurde, ist er nach Art. 39 Abs. 1 lit. b. DSGVO unter anderem dazu verpflichtet, die mit Verarbeitungsvorgängen betrauten Mitarbeiter zu sensibilisieren und zu schulen. Die Datensicherheit ist ein untrennbarer Bestandteil des Datenschutzes. Daher sollten im Rahmen von Schulung und Sensibilisierung auch in angemessenem Maß aktuelle Bedrohungen der IT-Sicherheit thematisiert werden.

**Schulen, schulen, schulen.** Dies bedeutet allerdings auch, dass eine einmal im Jahr stattfindende einstündige Schulung nicht immer ausreicht. Auch sollte man Lösungen eher kritisch sehen, bei denen sich Mitarbeiter online ein einstündiges Video ansehen und dafür eine bunte „Urkunde" erhalten. In aller Regel werden nämlich solche Videos nicht „tagesaktuell" sein. Ein verantwortungsvoller Datenschutzbeauftragter wird bei Schulungen jedoch stets auf die neuesten Bedrohungen eingehen.

Natürlich sind Schulungen online möglich. Diese müssen aktuell sein, und die Mitarbeiter müssen Fragen stellen können. Ein Datenschutzbeauftragter muss einschätzen können, ob zusätzliche Schulungen oder Informationen erforderlich sind, um die Mitarbeiter ausreichend zu sensibilisieren, und er muss dies auch der Geschäftsleitung mitteilen. Schließlich soll ein Datenschutzbeauftragter dabei unterstützen, Schaden vom Unternehmen, der Praxis oder Institution abzuwenden.

Wenn Schulungen zu Datenschutz und Datensicherheit/IT-Sicherheit sich seit dem Vorjahr nicht geändert haben, jedes Jahr die gleichen Folien verwendet werden und statt der Beschreibung aktueller Bedrohungen stets die drakonischen Strafvorschriften der DSGVO zitiert werden, wären grundsätzliche Änderungen sinnvoll.

Sind Mitarbeiter eher wenig IT-affin, wäre es sinnvoll, diese weiterzuqualifizieren und zu sensibilisieren oder aber die Tätigkeit dieser Mitarbeiter sowie deren Nutzerrechte so zu begrenzen, dass der Institution kein Schaden entstehen kann. Ein Mitarbeiter kann keinen schädlichen E-Mail-Anhang anklicken, wenn er keinen Zugang zu einem E-Mail-Konto hat.

**Ein- und Zugriffsmöglichkeiten begrenzen.** Sinnvoll ist es auch, das Recht, Einstellungen zu verändern oder Software zu installieren, auf einen Administrator zu begrenzen. So können unbefugte Nutzer erst gar kein Einfallstor für Schadprogramme öffnen. Generell sollte geprüft werden, ob jeder Mitarbeitende einen Zugang zu Internet und E-Mail benötigt oder ob nicht häufig ein Zugang zum Intranet einer Institution ausreichend ist.

Was schließlich den Umgang mit rücksichtslosen Personen angeht, sollte man die Möglichkeit prüfen, Zugriffe und Rechte einzuschränken. Darüber hinaus wird dringend empfohlen, vorsätzliche Verstöße gegen Richtlinien zu ahnden und mit angemessenen Sanktionen zu belegen. Wird Fehlverhalten im Zusammenhang mit der IT-Sicherheit geduldet, ist es häufig nur noch eine Frage der Zeit, bis eine Geldforderung Krimineller eingeht, weil Datenbestände abgeflossen oder verschlüsselt sind.

Allein durch Technik können Daten und Systeme jedoch nicht vollständig geschützt werden. Ein wirksamer Schutz ist nur im Zusammenspiel zwischen Technik und Nutzer dauerhaft möglich. Auch Verbote und Richtlinien sind nicht notwendigerweise ein Garant dafür, dass die IT-Sicherheit in einer Institution nicht gefährdet wird. Vielmehr ist es erforderlich, dass Mitarbeiter regelmäßig über aktuelle Bedrohungen informiert und geschult werden. Bedenkt man das Schadenspotenzial bis hin zum „Sudden Death" einer Institution, so sind die Kosten für diese Schulungen eine wichtige und zukunftssichernde Investition.

Natürlich sollte man Mitarbeiterinnen und Mitarbeiter keinesfalls als Bedrohung

## DAS WICHTIGSTE AUF EINEN BLICK

1. Technische Maßnahmen alleine reichen in aller Regel nicht, um die IT-Sicherheit dauerhaft zu gewährleisten.

2. Der Mensch muss als wesentlicher Faktor im Rahmen von Sicherheitskonzepten berücksichtigt werden.

3. Eine einstündige jährliche Schulung zum Datenschutz reicht in vielen Fällen nicht aus, um Mitarbeiter ausreichend für die Belange von Datenschutz und IT-Sicherheit (Datensicherheit) zu sensibilisieren. Der Schulungs- und Informationsbedarf der Mitarbeiter sollte unternehmensindividuell ermittelt werden.

4. Mangelnde Sensibilisierung der Mitarbeiter erhöht die Eintrittswahrscheinlichkeit von sicherheitsrelevanten Vorfällen signifikant.

5. Viele Probleme lassen sich vermeiden, wenn Mitarbeiter regelmäßig auf aktuelle Gefahren hingewiesen werden.

6. Schulungen sollten über aktuelle Gefährdungslagen informieren und interaktiv erfolgen, sodass Teilnehmer Fragen stellen und insbesondere auch konkrete Sachverhalte aus dem Berufsalltag einbezogen werden können.

7. Sinnvoll sind Beschränkungen der Zugriffs- und Einstellmöglichkeiten von Mitarbeitern sowie deren E-Mail- und Internetnutzung.

8. Der Verstoß von Mitarbeitern gegen Richtlinien des Datenschutzes und der Datensicherheit sollte konsequent geahndet werden. Ein „Datenschutzgegner" kann schwere Schäden verursachen, wenn er nicht frühzeitig in die Schranken gewiesen wird.

der IT-Sicherheit sehen. Sie können vielmehr einen Großteil möglicher Schadensfälle abwenden, wenn sie entsprechend gut geschult sind. Die Erfahrung des Autors zeigt, dass es in den Unternehmen, Praxen und Institutionen, in denen Mitarbeiter regelmäßig geschult und sensibilisiert werden, eher selten zu meldepflichtigen Problemen bei der IT-Sicherheit kommt. Treten größere Schadensereignisse auf, lässt sich dies häufig auf ein mangelhaftes Management von IT-Sicherheit und Datenschutz und insbesondere auch auf eine mangelnde Sensibilisierung von Mitarbeitern zurückführen.

## KONTAKT

Bei Fragen zur Schulung und Sensibilisierung von Mitarbeitern oder zu aktuellen Bedrohungen für die IT-Sicherheit steht der Autor gerne zur Verfügung. Eine telefonische Erstberatung erfolgt für Mitglieder der DGI e.V. kostenlos.

**Kontakt**:
dr.lenhard@it-planung.com
Tel: 06331 – 608–5501 (Büro)
0171 – 62 47 326 (Notfallnummer)

Wird trotz aller Vorsicht ein schädlicher E-Mail-Anhang angeklickt, kann in der Regel ein Abfluss von Daten oder ein Schaden am Datenbestand durch sofortige Maßnahmen geschulter Mitarbeiter abgewendet werden. Darum empfiehlt es sich, die regelmäßige Schulung als Baustein der IT-Sicherheit in das Konzept von Praxen und Institutionen aufzunehmen. Es steht zu vermuten, dass im Rahmen einer zukünftigen Überarbeitung der IT-Sicherheitsrichtlinie der KZBV auch der Faktor Mitarbeiter stärker als bislang darin berücksichtigt wird.

→ **Dr. Thomas H. Lenhard**