IT-Security-Awareness und die Managementebene

Lösungsorientierte Kommunikation

Das IT-Sicherheitsbewusstsein in deutschen Kliniken ist auch im Jahr 2020 ausbaufähig. Die Kluft zwischen erwünschter und gelebter Cybersicherheit ist nach wie vor sehr groß. Doch besonders im Gesundheitsbereich ist es zwingend notwendig, das gesamte Unternehmen über alle Hierarchieebenen hinweg regelmäßig für die Themen IT-Sicherheit und Online-Gefahren zu sensibilisieren.

Ein Hackerangriff auf die NASA im April 2018, bei dem sensible Daten gestohlen wurden, ist ein Paradebeispiel dafür, wie elementar die Schärfung des IT-Sicherheitsbewusstseins aller Mitarbeiter ist. Kritisiert wurde, dass die Sicherheits-Log-Tickets für mehr als sechs Monate unbearbeitet blieben. An dieser Stelle wird jede Führungskraft betonen, dass dies im Aufgabenbereich der IT-Abteilung liege und nicht in der Verantwortung einer Führungskraft – was durchaus richtig ist. Dennoch bleibt die Frage, ob der Diebstahl nicht durch einen entsprechend sensibilisierten Mitarbeiter hätte früher erkannt werden können. In der Studie „Digitalisierung in der Gesundheitswirtschaft" von Rochus Mummert aus dem Jahr 2018 wurde die Frage zur IT-Sicherheit in deutschen Kliniken gestellt. Obwohl knapp 43 Prozent der Teilnehmer angaben, dass ihr Krankenhaus bereits Ziel von Hackerattacken gewesen sei, hielten lediglich 38 Prozent der Befragten die verstärkte Sensibilisierung der Mitarbeiter für Cybersicherheit und Onlinegefahren durch gezielte Schulungen für wichtig.

Gerne setzen Mitarbeiter ihre privaten Endgeräte in der Firma ein, da die Oberfläche vertraut ist oder sie mehr Rechte für Installationen besitzen.

IT-Sicherheit: Wer trägt Verantwortung?

Doch wer trägt nun Verantwortung für die Wahrung der IT-Sicherheit in einem Unternehmen – die IT-Abteilung oder die jeweilige Führungskraft? Führungskräfte können keinesfalls selbst die eigenen Mitarbeiter in IT-sicherheitstechnischen Fragestellungen schulen. Dennoch sind sie von diesem wichtigen Thema nicht vollkommen unberührt. Im Gegenteil: Sie nehmen täglich eine entscheidende Vorbildfunktion ein. Ihnen obliegt es, ihren Mitarbeiter kontinuierlich einen adäquaten Umgang mit der IT vorzuleben und sie hinsichtlich IT-Sicherheit zu sensibilisieren. Zudem sollten sie für eine lösungsorientierte und reibungslose Kommunikation zwischen IT-Abteilung und der Belegschaft sorgen.

> „Die Aufgabe der Führungskraft ist es nun, eine lösungsorientierte Kommunikation sicherzustellen.
>
> Oliver Heitz

Lösungsorientierte Kommunikation sicherstellen

Kommunikative Barrieren beiderseits führen oftmals dazu, dass zwischen IT-Abteilung und nicht-IT-affinen Mitarbeitern der Informationsfluss nicht reibungslos funktioniert. So sind IT-Themen für einen Großteil der Mitarbeiter aufgrund des fachspezifischen Vokabulars nur schwer verständlich. Versuchen Mitarbeiter hingegen IT-Probleme zu beschreiben, kann bzw. möchte die IT-Abteilung diese nicht verstehen, da sie nicht technisch hinreichend formuliert sind. Die Aufgabe der Führungskraft ist es

Bild: tetxu (stock.adobe.com)

nun, eine lösungsorientierte Kommunikation sicherzustellen. Dies gelingt jedoch nur, wenn ein gewisses Grundverständnis für Cybersecurity vorhanden ist. Auf folgende Themen können Führungskräfte Einfluss nehmen, ohne sich tiefgreifende IT-Kenntnisse aneignen zu müssen. Diese Themen sollten zudem regelmäßig fester Bestandteil von Abteilungsbesprechungen sein.

Auf diese Themen können Führungskräfte Einfluss nehmen

- **Phishing-Mails erkennen:** Hierbei handelt es sich um unscheinbare Websites oder Kurznachrichten, die den Spamfilter bzw. die Firewall der Firma überwunden haben. Harmlos wirkende E-Mails, die eventuell sogar vertraute Absender oder Ansprachen verwenden, locken den Leser, auf einen Link zu klicken. Hinter diesem Link verbergen sich aber Trojaner, die durch simples Anklicken aktiviert werden und so ins Firmennetzwerk gelangen.
- **Unbedachte Installation von Apps verhindern:** Gerne werden Mitarbeiter beim Surfen im Internet dazu aufgefordert, eine App zu installieren. Was im privaten Bereich einfach und üblich ist, ist für das Firmennetzwerk ein Problem. Da die Installation vom User ausgelöst wird, reagieren die firmeneigenen Sicherheitswerke häufig nicht oder erst zu spät.
- **Weitergabe von persönlichen Daten reduzieren:** Durch das übermäßige Registrieren für Newsletter oder Websites werden persönliche Daten weitergegeben und Cookies zugelassen. Hierdurch wird eine direkte Verbindung zum User hergestellt und dieser kann nun per Mail auf sehr persönliche Weise angeschrieben werden. Phishing-Mails werden so noch professioneller und können kaum als solche erkannt werden.
- **Nutzung von Private Devices im Firmennetzwerk besser regeln:** Gerne setzen Mitarbeiter ihre privaten Endgeräte in der Firma ein, da die Oberfläche vertraut ist oder sie mehr Rechte für Installationen besitzen. Solange sich diese Geräte in einem Gast-WLAN des Unternehmens befinden, ist das unproblematisch. Kritisch wird es, wenn sie in das Firmen-Netzwerk eingebunden werden. Auf diese Weise werden alle Sicherheitsvorkehrungen schnell außer Kraft gesetzt.
- **Weiterleiten von E-Mails untersagen:** Werden dienstlich relevante Informationen über private Netzwerke verarbeitet, die dann wiederum in Firmenserver eingespielt werden, entsteht ebenfalls ein erhöhtes Risiko. Spamfilter erkennen private Mailadressen als „vertrauensvolle Quelle“ und lassen die Weiterleitung zu. Solche E-Mails werden von der Firewall gescreent, Anhänge und Links werden allerdings ungeprüft durchgereicht, was wiederum einen ungewollten Zugang von außen auslösen kann.

IT-Sicherheit: Ein kontinuierlicher Prozess aller Beteiligten

Abschließend lässt sich zusammenfassen, dass IT-Sicherheit nicht einzig und allein in der Verantwortung einer Abteilung oder eines einzelnen Mitarbeiters liegt. Vielmehr ist dies eine gemeinsame Aufgabe aller Beteiligten, da nur die Gesamtheit aller Erkenntnisse im Sinne von Schwarmintelligenz den größtmöglichen Schutz erzeugen kann. Auf Entscheiderebene liefert hierbei die kontinuierliche Sensibilisierung der eigenen Mitarbeiter anhand aktueller und konkreter Beispiele den entscheidenden Beitrag zur Steigerung der Cyber-Sicherheit.

Oliver Heitz

Partner der Rochus Mummert Healthcare Consulting GmbH,
Kontakt: Oliver.Heitz@Rochus-Mummert.com

Bild: privat