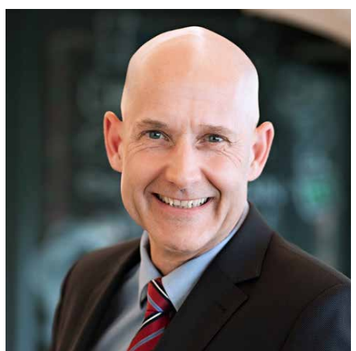
Modul um Modul zur menschlichen Firewall

Durch den immer breiteren Einsatz von Informations- und Kommunikationstechnologien in der Hotellerie und Gastronomie kommt den sicherheitsrelevanten Aspekten eine sehr hohe Bedeutung zu. Mit der Zunahme der Digitalisierung steigen auch die damit zusammenhängenden Gefahren. Die SHL Schweizerische Hotelfachschule Luzern trägt dieser Entwicklung im neuen Lernfeld «ICT Security» (Informationssicherheit) Rechnung. Die angehenden Führungspersönlichkeiten der Branche werden für diese brisante Thematik sensibilisiert

Erfahrungsbericht von Heiko Siebert*, SHL-Dozent

Immer häufiger erreichen uns Berichte über Hacker-Angriffe auf Hotels und Restaurants, was ein verstärktes Handeln zur Sicherheit in diesem Bereich erfordert. Zum einen braucht es technisch ausgereifte Konzepte und Schutzmassnahmen wie Virenschutz oder Firewall durch einen ICT-Partner. Zunehmend sind jedoch auch Pläne für mögliche Ernstfälle notwendig, sowie Massnahmen, um das Sicherheitsbewusstsein der Mitarbeitenden zu schärfen. Diesen Handlungsbedarf für zukünftige Unternehmer:innen in Hotellerie, Gastronomie, Tourismus und anderen Dienstleistungsbranchen hat die SHL Schweizerische Hotelfachschule Luzern erkannt. Seit September 2022 wird – in Kooperation mit der arcade solutions ag und Knowbe4 – die Thematik ICT Security in den SHL-Bildungsgängen integriert behandelt.



Heiko Siebert sensibilisiert angehende Hoteliers und Hotelièren für Cyber-Risiken

Eigenes Verhalten prüfen

Ziel der Unterrichtseinheiten ist zunächst die Sensibilisierung der Studierenden auf Risiken und Gefahren im eigenen Umgang mit dem Internet sowie digitalen Produkten und Anwendungen. Ausgehend vom persönlichen Verhalten und den erkannten Risiken, werden Schlüsse und Erkenntnisse für die zukünftigen Rollen als Führungsperson gezogen.

Inhaltlich werden im ersten Modul Themen wie Passwörter, Social Engineering oder Phishing angesprochen. Die Studierenden befassen sich mit Fragen wie «Welche Passwörter sind sicher?» oder «Wie häufig sollte ich das Passwort wechseln?». Im Zusammenhang mit Social Engineering – bei dem Hacker Mitarbeitende in einem Unternehmen so manipulieren, dass diese vertrauliche Informationen preisgeben – werden verschiedene Praktiken dieses Angriffsvektors betrachtet. Ausserdem werden die Studierenden zweimal mit simulierten Phishing-Attacken getestet.

Die Ergebnisse daraus werden mit der Klasse geteilt und diskutiert. Die Studierenden erkennen dabei ihre eigene Anfälligkeit sowie einen oft leichtsinnigen Umgang mit E-Mails und digitalen Informationen. Anlässlich der letzten Durchführung waren sie insbesondere erstaunt, wie leicht es ist, scheinbar sichere Absender zu nutzen, um einen Cyber-Angriff aufzuführen.

Digitale Sicherheit im Unternehmen

Im zweiten Modul werden Massnahmen zur Erhöhung der digitalen Sicherheit auf Unternehmensseite thematisiert. Dabei gibt ein spezialisierter Security-Ingenieur tiefere Einblicke in Gefahren, die für ein Unternehmen bestehen. Die Bedrohungslandschaft, der Hotels und Restaurants in diesem Bereich ausgesetzt sind, gestaltet sich äusserst vielfältig. Gemäss dem Sicherheitsunternehmen Watchguard geht das grösste Risiko von Datenschutzverletzungen, Ransomware (Schadsoftware), Phishing-Attacken, anfälligen WLAN-Netzwerken und Zugriffen auf sensible Daten von Gästen und Mitarbeitenden aus.

Die erste Durchführung der anwendungsorientierten und brandaktuellen «ICT Security»-Module an der SHL Schweizerischen Hotelfachschule Luzern wurde von den Studierenden sehr positiv aufgenommen. Bei vielen Teilnehmenden war das Vorwissen in diesem Bereich gering. Die Bedeutung der Inhalte, sowohl für das private wie auch für das berufliche Umfeld als zukünftige Unternehmer:innen, wurde erkannt und die Sensibilisierung auf diesem Gebiet geschätzt. Nicht zuletzt fühlen sich die Teilnehmenden nun sicherer und besser gewappnet gegen Cyberattacken.

ICT Security im Unterricht – wichtiger denn je: Die NCSC vermeldet über 700 Cyberangriffe jede Woche.

Was ist beim Passwort zu beachten

- Passwörter mit mehr als 12 Zeichen wählen.
- Keine einfach zu erratenden Passwörter (z. B. persönliche Namen und Daten, Wörter aus dem Wörterbuch oder Tastaturfolgen) einsetzen.
- Das gleiche Passwort nicht mehrfach verwenden.
- Willkürliche Wortkombinationen (auch Passphrasen genannt) als Passwort wählen
- und mit Sonderzeichen anreichern (z. B. Bindestrich zwischen Wörtern oder Buchstabe a mit @ ersetzen).