IT-Sicherheit für Berufsschüler

Projekt „Bottom-Up“ trägt Wissen in Unternehmen

Gruppenarbeit im Unterricht

Besonders kleine und mittelständische Unternehmen tun sich beim Thema IT-Sicherheit oft schwer. Weil die Bewältigung der täglich anfallenden Arbeitsaufträge bereits alle Kapazitäten bindet, bleibt für präventive Maßnahmen wie Datensicherung, aber auch nötige Mitarbeiterschulungen meist wenig Zeit. Durch das Projekt „Bottom-Up“ von Deutschland sicher im Netz e. V. soll sich das ändern: Im Rahmen des Berufsschulunterrichts werden den Auszubildenden der Betriebe wichtige Inhalte rund um die Internetsicherheit im Unternehmen vermittelt. Nach einer elfmonatigen Pilotphase startet das Projekt nun bundesweit durch. Projektleiter Sascha Wilms erklärt, warum Bottom-Up nachhaltig wirken kann.

Das englische Bottom-Up steht dabei sowohl für „von unten nach oben“ als auch für die umgangssprachliche Floskel „den Hintern hochkriegen“. „Durch das Projekt sollen die Beschäftigten von morgen für die Herausforderungen einer digitalen Sicherheitskultur sensibilisiert werden. Viele Studien zeigen, dass die Beschäftigten in Unternehmen immer noch eine große Schwachstelle darstellen. Hier möchten wir möglichst früh ansetzen“, erklärt Wilms. Im Rahmen des Projekts wurden Unterrichtsmaterialien entwickelt, die Berufsschullehrer im Unterricht einsetzen können. „Es gibt Lehrerskripte, damit die Lehrenden sich gut auf die Vermittlung des fachfremden und niedrigschwelligen Stoffes vorbereiten können. Außerdem kommen Vorschläge hinzu, wie sie den Unterricht minutengenau gestalten und welche methodischen Ansätze genutzt werden können. Trotzdem bleibt immer noch genug Raum für die eigene Gestaltung“, so der Projektleiter.

Lebensnahe Themen

In verschiedenen Lerneinheiten werden grundlegende Kenntnisse aus dem Bereich der IT-Sicherheit in Unternehmen aufgearbeitet, wie etwa Datenschutz, Sicherheit für mobile Endgeräte, die sichere Nutzung einer Cloud, Datensicherung oder auch sichere E-Mail-Kommunikation. „Die Grenzen zwischen betrieblicher und privater Nutzung sind oft fließend. Die Themen sind daher so gewählt, dass die Schülerinnen und Schüler das angeeignete Wissen auch für den privaten Gebrauch anwenden können – das macht das Thema umso attraktiver“, betont Wilms. Auch auf gängige Angriffstechniken wird eingegangen, etwa auf das so genannte „Social Engineering“, bei dem Betrüger versuchen, über die

Beschäftigten eines Unternehmens an sensible Geschäftsdaten zu kommen. „Auch private Social-Media-Kanäle von Mitarbeitern sind dabei im Fokus von Kriminellen. Sie suchen den Kontakt, um darüber Betriebsgeheimnisse auszuspionieren“, erklärt der Experte.

Folgende Artikel könnten Sie auch interessieren:

- Der digitale Nachlass
- Erste-Hilfe-App bei Cybermobbing
- Daten richtig löschen

Alle Artikel dieser Kategorie

Weitere Infos für Lehrer / Erzieher

„Die Beweispflicht bleibt“

Das neue Sexualstrafrecht

Im Juli 2016 hat der Bundestag Änderungen im Sexualstrafrecht... [mehr erfahren]

Behinderung von Rettungskräften ist kein Kavaliersdelikt

Unfall-Gaffer müssen mit Strafen rechnen

Szenen mit Schaulustigen, die verunglückte Personen nach Unfällen... [mehr erfahren]

Kinder- und Jugendarbeit beim THW

Spielend helfen lernen

Das Technische Hilfswerk (THW) unterstützt die Rettungskräfte von... [mehr erfahren]

Sich im Ernstfall wehren können

Selbstverteidigung für Kinder

Sich im Notfall selbst verteidigen zu können, gibt einem ein sicheres... [mehr erfahren]

Zwischen Ermittlungsgrundlage und Datenschutz

Vorratsdatenspeicherung – ja oder nein?

Die Speicherung von Verkehrsdaten, also der Aufzeichnung wesentlicher... [mehr erfahren]
