KEEPER®

Cybersicherheit in Schulen

Schutz der Schüler im digitalen Zeitalter

Überblick

Da Schulen zunehmend digitale Hilfsmittel wie Lernplattformen, virtuelle Klassenzimmer und vernetzte Geräte einsetzen, wird die Technologie zu einem zentralen Bestandteil der modernen Bildung. Der rasche digitale Wandel des 21. Jahrhunderts bringt jedoch auch neue Risiken für die Cybersicherheit mit sich, die Bildungseinrichtungen nicht ignorieren dürfen.

Der Keeper Security Report 2024, der aus einer Studie unter 6.000 Personen in Australien, Neuseeland, Singapur, Indonesien, Japan, Frankreich, dem Vereinigten Königreich, den USA und der DACH-Region hervorgegangen ist - gleichmäßig verteilt auf Schüler ab 16 Jahren, Eltern und die allgemeine Bevölkerung - zeigt eine kritische Lücke zwischen dem Vertrauen und der Realität in der Fähigkeit der Schulen, Schüler im digitalen Zeitalter zu schützen.

Während viele Eltern glauben, dass die Schulen sensible Daten schützen, setzen schwache oder wiederverwendete Passwörter und eine begrenzte Ausbildung in die Cybersicherheit die Schüler ständigen Bedrohungen wie Datenschutzverletzungen, Identitätsdiebstahl und Betrug aus. Die Ergebnisse unterstreichen die dringende Notwendigkeit für Schulen und Familien, gemeinsam stärkere digitale Sicherheitsmaßnahmen zu ergreifen und die Schüler für Online-Risiken zu sensibilisieren.

Aktuelle Cybersicherheitspraktiken in Schulen

Die Umfrage von Keeper Security zeigt eine gemischte Landschaft bei den Cybersicherheitspraktiken in Schulen. Zwar vertrauen 74 % der Eltern darauf, dass die Schule ihres Kindes sensible Daten schützt, doch stimmt dieses Vertrauen nicht mit den schulischen Praktiken überein. Nur 21 % der Eltern geben an, dass ihre Schulen Anleitungen zur Erstellung und Verwaltung sicherer Passwörter geben, was zu gefährlichen Passwortgewohnheiten beiträgt. So erläuterten 19 % der Befragten beispielhaft, dass sie Passwörter für private und schulische Konten wiederverwenden, was das Risiko einer weitreichenden Sicherheitsverletzung erhöht.

Vertrauen in die Cybersicherheitsmaßnahmen der Schule

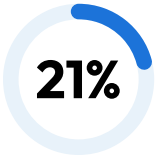
18% **Sehr zuversichtlich**

56% **Etwas zuversichtlich**

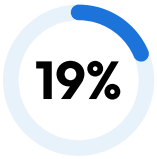
22% **Nicht sehr zuversichtlich**

4% **Überhaupt nicht zuversichtlich**

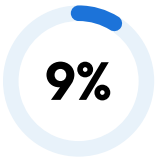
Praktiken der Passwortverwaltung



Schulen geben Anleitungen zu sicheren Passwörtern



Wiederverwendung von Passwörtern zwischen Konten



Schulen bieten Zugriff auf einen Passwortmanager

Die begrenzte Verfügbarkeit von sicheren, digitalen Passwortmanagern – nur 9 % der Schulen bieten Zugriff darauf – verschärft diese Risiken noch weiter. Passwortmanager, die für die sichere Erstellung und Speicherung komplexer Passwörter unverzichtbar sind und von Regierungsbehörden und Cybersicherheitsexperten empfohlen werden, sind nicht vorhanden. Dies stellt eine klare Möglichkeit dar, wie Schulen ihre Cybersicherheitspraktiken erheblich verbessern könnten.

Die Notwendigkeit einer verbesserten Cybersicherheitsausbildung

Die Aufklärung über Cybersicherheit in Schulen ist gefährlich dürftig: Nur 14 % der Schulen schreiben Schulungen zur Sensibilisierung für Sicherheit vor, weitere 13 % bieten sie optional an. Der begrenzte Umfang der obligatorischen Schulungen bedeutet, dass viele Familien keine aktuellen Informationen über die Online-Sicherheit erhalten. Dadurch sind die Schüler den sich entwickelnden Cyberbedrohungen schutzlos ausgeliefert. Wirksame Schulungen zur Cybersicherheit sollten sich nicht nur darauf konzentrieren, wie man Phishing-Betrügereien erkennt, Maßnahmen zum Schutz von Geräten ergreift und die Bedeutung regelmäßiger Software-Updates versteht, sondern auch auf den sicheren Umgang mit dem digitalen Fußabdruck der Schüler.

Die Aufklärung der Schüler über die Auswirkungen ihrer Online-Aktivitäten, z. B. Beiträge in sozialen Medien und Surfgewohnheiten, ist der Schlüssel zum Schutz ihrer persönlichen Daten. Bei der Aufklärung über Cybersicherheit sollte beispielsweise darauf hingewiesen werden, wie wichtig es ist, die Einstellungen der Privatsphäre auf Social-Media-Plattformen so anzupassen, dass die öffentliche Darstellung begrenzt wird. Die Aufklärung der Schüler darüber, wie böswillige Akteure ihren digitalen Fußabdruck ausnutzen können, um in Zukunft einen Identitätsdiebstahl oder gezielte Angriffe durchzuführen, ist entscheidend für die Förderung eines verantwortungsvollen Online-Verhaltens.

Auswirkungen von Cybersicherheitsvorfällen auf Schulen

Cyberangriffe auf Bildungseinrichtungen können schwerwiegende und weitreichende Folgen für Schüler, Lehrkräfte und Verwaltungsangestellte gleichermaßen haben. Dies unterstreicht die Notwendigkeit von robusten Sicherheitsmaßnahmen zum Schutz von Konten und sensiblen Daten. Der Umfrage zufolge geben zwar nur 7 % der Befragten an, dass die Bildungseinrichtung ihres Kindes oder ihre eigene Einrichtung schon einmal gehackt wurde, doch die Auswirkungen sind erheblich. Auf die Frage nach den Effekten solcher Verletzungen gaben die Befragten die folgenden Auswirkungen an:

32%
Datendiebstahl

24%
Identitätsdiebstahl

26%
Gestohlene Anmeldeinformationen

27%
Kompromittierte Konten

16%
Finanzielle Auswirkungen auf die Schule

14%
Finanzielle Auswirkungen auf Schüler/Mitarbeiter

Das Ausmaß des Daten- und Identitätsdiebstahls macht deutlich, dass sowohl die Privatsphäre als auch die Sicherheit der Institutionen ernsthaft gefährdet sind. Die Häufigkeit gestohlener Anmeldeinformationen und kompromittierter Konten veranschaulicht den großen Schaden, den solche Verstöße anrichten können. Oftmals werden dabei sensible Informationen offengelegt. Obwohl über die finanziellen Auswirkungen weniger häufig berichtet wird, sind sie sowohl für Schulen als auch für Einzelpersonen nach wie vor beträchtlich und zeigen, dass Cyberangriffe Schäden verursachen können, die über die unmittelbaren Daten- und Identitätsprobleme hinausgehen.

Die Rolle von Familien bei der Cybersicherheit

Eltern und Erziehungsberechtigte spielen eine wichtige Rolle bei der Stärkung der Cybersicherheitspraktiken zu Hause. Die Umfrage von Keeper zeigt jedoch, dass 19 % der Familien Passwörter wiederverwenden – eine gefährliche Praxis, die dazu führen kann, dass mehrere Konten durch Credential Stuffing-Angriffe kompromittiert werden. Während viele Schulen keine ausreichenden Ressourcen für die Cybersicherheit bereitstellen, können Familien dazu beitragen, die Lücke zu schließen, indem sie starke, eindeutige Passwörter und die Multifaktor-Authentifizierung (MFA) verwenden. MFA fügt eine zusätzliche Sicherheitsebene zu Online-Konten hinzu, indem es mindestens eine zusätzliche Form der Verifizierung für die Anmeldung verlangt.

Mehr als die Hälfte (51 %) der Befragten geben an, dass sie sehr oder eher besorgt über die Cybersicherheit in der Schule sind. Das macht deutlich, dass die Eltern sich der Risiken bewusst sind, auch wenn die Cybersicherheitspraktiken möglicherweise nicht ausreichen. Um diesen Risiken entgegenzuwirken, sollten Familien die Online-Aktivitäten ihrer Kinder proaktiv überwachen und sich zu Hause an bewährte Praktiken der Cybersicherheit halten. Dazu gehört, dass man lernt, verdächtige E-Mails und Links zu erkennen, starke und eindeutige Passwörter zu verwenden, MFA für alle Konten zu aktivieren, die dies ermöglichen, und die Software regelmäßig zu aktualisieren, um vor bekannten Sicherheitslücken zu schützen.

Nach vorne schauen: ein einheitlicher Ansatz für die Cybersicherheit

Um die Messlatte für die Cybersicherheit in unseren Schulen höher zu legen, bedarf es gemeinsamer Anstrengungen sowohl der Bildungseinrichtungen als auch der Familien der Schüler, die sie besuchen. Die Schulen müssen ihre Programme zur Aufklärung über Cybersicherheit verbessern: Sie müssen bewährte Tools wie Passwortmanager einbeziehen und Schulungsinitiativen ausweiten, um bewährte Verfahren zur Cybersicherheit abzudecken. Die Familien sollten diese Bemühungen unterstützen, indem sie zu Hause gute Cybersicherheitsgewohnheiten fördern und sich aktiv an der digitalen Erziehung ihrer Kinder beteiligen.

Durch die Zusammenarbeit können Schulen und Familien eine sicherere Online-Umgebung für Schüler schaffen, die den Nutzen des technologischen Fortschritts maximieren und gleichzeitig die damit verbundenen Cyberrisiken minimieren können.

Methodik

Diese Online-Umfrage unter 6.000 Befragten in Australien, Neuseeland, Singapur, Indonesien, Japan, Frankreich, dem Vereinigten Königreich, den USA und der DACH-Region wurde vom Marktforschungsunternehmen OnePoll in Übereinstimmung mit dem Verhaltenskodex der Market Research Society durchgeführt. Diese Umfrage wurde vom Forschungsteam von OnePoll beaufsichtigt und bearbeitet. OnePoll ist MRS Company Partner, Unternehmensmitglied von ESOMAR und Mitglied des British Polling Council.