

Interview

Wie sicher ist der digitale Schulalltag?

[05.08.2022] Datensicherheit ist beim Thema Bildungsdigitalisierung einer der wichtigsten Aspekte, stellt Schulen aber immer noch vor Herausforderungen. Wie sie diesen am besten begegnen können, erklären im Interview Philip Heimes, Chief Technology Officer bei Sdui, und Philip Saladin, Head of Sales Switzerland, bei der Deutschen Gesellschaft für Cybersicherheit (DGC).

Herr Heimes, Herr Saladin, Sicherheit ist in Schulen ein besonders sensibles Thema. Aus der analogen Welt sind Sicherheitsmaßnahmen ganz selbstverständlich: Wir lassen keine Schulfremden in die Klassenzimmer, das Schulgebäude wird nach Schulschluss abgeschlossen und wichtige Dokumente werden zum Beispiel im Sekretariat verschlossen. Im digitalen Bereich gibt es diese Selbstverständlichkeit noch nicht. Was verstehen Sie als Experten unter Cyber-Sicherheit an Schulen?

Philip Saladin: Ganz allgemein geht es beim Thema Cyber-Sicherheit um den Schutz von Daten. Im Bereich Schule sind das im Speziellen: Persönliche Daten wie Name, Geburtsjahr, der Wohnort von Schülerinnen und Schülern, Noten, Klassenbucheinträge, Zeugnisse oder Stundenpläne. All diese Informationen werden als Daten auf Festplatten, Servern oder in einer Cloud gespeichert. Auch die gesamte digitale Kommunikation innerhalb der Schulgemeinschaft gehört zu den sensiblen Daten. Es gehört zum Alltag von Schulen, dass Daten erhoben, verarbeitet, übertragen, gespeichert, archiviert und gelöscht werden. Deshalb ist es auch ihre Aufgabe, diese vor Missbrauch zu schützen.

Philip Heimes: Cyber-Sicherheit an Schulen muss einen genauso hohen Stellenwert haben, wie andere analoge Sicherheitsmaßnahmen, die für uns selbstverständlich sind. Ausgedruckte Zeugnisse beispielsweise würden niemals offen und für jeden einsehbar herumliegen. Einen unachtsamen Umgang mit personenbezogenen Daten würden wir als massiven Verstoß gegen die Persönlichkeitsrechte eines Kindes werten. Bei digitalen Daten kommt es hingegen immer noch häufig vor, dass genau solche unachtsamen Verstöße passieren. Oft wissen die Beteiligten gar nicht, dass sie mit ihren Handlungen Risiken eingehen und sich einer Gefahr aussetzen. Unwissenheit und das Gefühl, im riesigen Feld der Schuldigitalisierung mit solchen Fragen alleingelassen zu werden, stellen ein Problem dar. Darüber wollen Sdui und die DGC aufklären. Die pandemiebedingten Zeiten von Homeschooling sind weitgehend vorbei.

Welchen Stellenwert hat das Thema Cyber-Sicherheit aktuell überhaupt noch in der Schule? Wird dies bei der Vielzahl anderer Herausforderungen nicht überbewertet?

Philip Heimes: Ich denke, es ist nicht mehr zeitgemäß, das Thema Schuldigitalisierung auf Videokonferenzen im Homeschooling zu reduzieren. Wir sehen bei den rund 5.000 Schulen, welche die Plattform Sdui nutzen, dass sich der Umgang mit digitalen Daten wie ein roter Faden durch den Alltag zieht. Heute fragt niemand mehr, ob digitalisiert werden soll, sondern wie. Schulen sind in der Krise zu Gestaltern der digitalen Transformation geworden. Jetzt gilt es, aus der Not eine Tugend zu machen. Das heißt für mich, Kompetenz im Bereich der Cyber-Sicherheit zu schaffen, um Risiken bewerten zu können. Das Thema Sicherheit in Verbindung mit der Digitalisierung kann dabei gar nicht hoch genug bewertet werden.

„Jeder Mitarbeiter, der im Bereich der Security Awareness geschult ist, stellt einen Mehrwert da.“
Die Deutsche Gesellschaft für Cybersicherheit berät Unternehmen wie Behörden in Fragen der Cyber-

Sicherheit. Was sind aus Ihrer Erfahrung die größten Sicherheitsrisiken für Organisationen?

Philipp Saladin: Laut einer Befragung des Branchenverbands Bitkom aus dem Jahr 2021 ist bei deutschen Unternehmen in 31 Prozent der Fälle die Infizierung mit Schad-Software wie etwa Ransomware-Attacken das größte Risiko. So genannte DDoS-Attacken, bei denen Angreifer bestimmte Ressourcen gezielt überlasten und zum Beispiel Server mit massenhaften Anfragen in die Knie zwingen, betrafen 27 Prozent. Spoofing, das Vortäuschen einer falschen Identität, und Phishing, das Beschaffen persönlicher Daten mithilfe von gefälschten E-Mails, haben in 20 beziehungsweise 18 Prozent der Unternehmen Schäden verursacht.

Und was sind aus Ihrer Sicht die größten Sicherheitsrisiken für Schulen?

Philip Saladin: Wie in Unternehmen gilt auch in Schulen: Der Mensch stellt das größte Sicherheitsrisiko dar. Das fängt bei Passwörtern an, die auf Zettel geschrieben werden oder als Post-it am Bildschirm kleben. In der Schule sind es auch unterschiedliche, private Geräte, die genutzt werden, wenn es kein zentrales Device-Management gibt. Aber auch fremde USB-Sticks, die verwendet werden, stellen immer noch ein Sicherheitsrisiko dar. Die größten Sicherheitslücken entstehen allerdings, wenn Software-Updates und Sicherheits-Patches nicht durchgeführt werden. Über 50 Prozent der hoch sicherheitsrelevanten Schwachstellen könnten durch Updates geschlossen werden.

Was können die Folgen von Angriffen und Datenlecks sein?

Philip Saladin: Im Bildungswesen können bei unsachgemäßer Bearbeitung solcher Daten beispielsweise Diskriminierungen und Einschränkungen bei der Wahl der Ausbildung und des Berufs denkbar sein. Oder aber eine Schule wird mittels einer Ransomware-Attacke verschlüsselt und kann den Fortbetrieb der Schule nicht mehr gewährleisten. Plötzlich wird sie mit Lösegeldzahlungen und einem potenziellen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) konfrontiert.

Philip Heimes: Am schlimmsten ist es aus meiner Sicht, wenn persönliche Schicksale von Kindern mit einer Sicherheitslücke einhergehen – vertrauliche Informationen über einen Schüler, die dann im Internet landen, weiterverbreitet werden und vielleicht sogar für Mobbing genutzt werden. Solche Fälle sind leider Realität und auch Lehrkräfte können betroffen sein. Wer Opfer von Cyber-Kriminalität wird, hat damit oft schwer und lange zu kämpfen.

Wie können sich die Schulen schützen?

Philipp Saladin: Aus unserer Erfahrung weiß ich: Jeder Mitarbeiter, der im Bereich der Security Awareness geschult ist, stellt einen Mehrwert da. Ganz niederschwellige Tipps, die sehr viel bewirken können, sind: Öffnen Sie niemals Anhänge in E-Mails von unbekannten Dritten. Klicken Sie nie auf Links, welche auf dubiose Websites verweisen. Beim Verlassen Ihres Arbeitsplatzes sperren Sie immer Ihren Computer. Nutzen Sie keine USB-Sticks, welche Sie vermeintlich als Werbezwecke erhalten haben. Tipps für die IT im Speziellen sind: Nutzen Sie einen Schwachstellen-Scanner, welcher Ihre Netzwerkumgebung 24/7 überprüft. Führen Sie Software-Updates und Sicherheits-Patches umgehend nach Freigabe der Hersteller aus.

Philip Heimes: Ich denke, ein ganz wichtiger Schritt ist, überhaupt ein Bewusstsein für das Thema Cyber-Sicherheit zu schaffen. Jeder in der Schulgemeinschaft kann einen Teil dazu beitragen, die Schule datensicher zu machen. Aber natürlich ist das Ganze auch eine Budgetfrage, denn in der Regel gibt es in der Schule nicht das notwendige Know-how und die Ressourcen, um die Systeme sicher zu machen und kontinuierlich zu überprüfen. Die Zusammenarbeit mit externen Experten wie der DGC, die bei der

Umsetzung von Strategien helfen können, bietet sich auch für Bildungseinrichtungen an. Und: Schulen sollten mit digitalen Lösungen arbeiten, die Sicherheit in der Schule ernst nehmen. Sdui tut das – uns ist das Thema Sicherheit beim Bau unserer Plattform besonders wichtig.

Sdui ist eine Plattform für digitale Kommunikation und Organisation an Schulen – wie sieht es mit der Sicherheit auf der Plattform aus?

Philip Heimes: Sdui ist DSGVO-konform und nutzt deutsche Server. Schulen, die die Plattform nutzen, müssen sich keine Sorgen darüber machen, wo die Daten gespeichert werden und ob ein Konzern im Ausland Schülerdaten abgreift. Sdui wurde gemeinsam mit Schulen in Deutschland konzipiert und wird im Austausch mit ihnen permanent weiterentwickelt. Uns ist dabei ein holistischer Ansatz von Datensicherheit wichtig, was bedeutet: Alle in der Schulgemeinschaft beteiligten Akteure müssen sich sicher auf der Plattform bewegen und miteinander kommunizieren können – Lehrkräfte, Schüler und Eltern.

Sdui und die DGC wollen in Zukunft miteinander kooperieren, um über Cyber Security an Schulen aufzuklären. Was bedeutet das konkret?

Philip Saladin: Sdui und die DGC sind zwei starke Partner, die gemeinsam für das Thema Cyber-Sicherheit sensibilisieren möchten. Wir kennen die Risiken der Digitalisierung und können Lösungen aufzeigen. In Zukunft wollen wir zum Beispiel Informationen und Tipps für Schulen zusammenstellen.

Philip Heimes: Uns geht es darum, Schulen und Bildungseinrichtungen zu befähigen, Risiken selbst zu erkennen und die Datensicherheit selbst beurteilen zu können. Ein Bewusstsein dafür zu schaffen, ist der erste Schritt. Und auch zu wissen, wo es Hilfe gibt. Wir finden es wichtig, Schulen mit dem bedeutsamen Thema Datensicherheit nicht allein zu lassen. Denn: Wir alle können dazu beitragen, das Internet jeden Tag etwas sicherer für uns und unsere Kinder zu machen.

()

Stichwörter: Schul-IT, Datenschutz, IT-Sicherheit, Sdui, DGC