„Uns fehlen Geräte und Personal“

IT-Sicherheit an Hochschulen

| IM GESPRÄCH | **Der Verein der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ (ZKI) hat die IT-Sicherheit an Hochschulen seit Jahren im Blick. Wie bewertet ein Experte aus der Informationssicherheit die aktuelle Lage an den Hochschulen?**

Forschung & Lehre: Herr Professor Paul, potenzielle Hackerangriffe sind heikel für Hochschulen, die eine Menge personenbezogener und Forschungsdaten verarbeiten. Wie oft kommt es zu unbefugten Zugriffen auf Hochschulnetzwerke?

Manfred Paul: Verbindungsversuche gibt es laufend. Meist werden sie automatisch durch Firewalls geblockt. Sogenannte Phishing-Attacken über E-Mails tauchen am häufigsten auf. Solche E-Mails erreichen einzelne Hochschulen mehrmals monatlich. Die Mails suggerieren dem Empfänger, dass sie von einem bekannten Absender kommen, das kann zum Beispiel ein bekannter Anbieter einer Dienstleistung sein wie die Post oder sogar ein anderer Hochschulmitarbeiter. Der Empfänger wird per Link auf eine Webseite gelenkt, auf der dann Login-Daten abgefragt werden, die später für andere Angriffe verwendet werden könnten. Von solchen Webseiten kann im Hintergrund Schadsoftware auf den Rechner landen, teilweise senden Hacker den sogenannten Schadcode auch gleich direkt als Mailanhang.

Professor **Manfred Paul** *ist Sprecher des Arbeitskreises Informationssicherheit des ZKI und Professor an Elektrotechnik und Informationstechnik an der Hochschule München..*

F&L: Konnten darüber schon Forschungsdaten oder personenbezogene Daten aus den Hochschulen abgegriffen werden?

Manfred Paul: Das ist schwer einzuschätzen und festzustellen, bekannt gewordene Logindaten werden natürlich sofort geändert, sofern die Nutzer das überhaupt selbst bemerken. Einzelne sogenannte Ransomware-Attacken haben teilweise zur Datenverschlüsselung von einzelnen Rechnern geführt. Diese Daten können jedoch in der Regel durch Backups wiederhergestellt werden. Persönlich ist mir kein Fall bekannt, bei dem eine Wiederherstellung – zumindest zum Zeitpunkt des letzten Backups – nicht möglich war.

F&L: Aus welchen Ländern kommen die meisten Angriffe?

Manfred Paul: Die meisten versuchten Zugriffe stammen von Systemen aus Russland, dem asiatischen Raum und dem Nahen Osten. Wir reden hier von Angeboten „as a service“: Angreifer nutzen teilweise Plattformen und sogenannte Botnetze, die im Darknet zur Miete angeboten werden. Wer im Einzelfall dahinter steckt, ist meist nicht feststellbar. Das unterscheidet sich je nach der aktuellen Politik in den einzelnen Ländern, aber sicher auch nach Geschäftsinteressen. Wir sprechen also nicht mehr von einzelnen Hackern, die irgendwo mit viel Zeit oder Langeweile sitzen und Cyberangriffe planen, sondern von Wirtschafts- und Industriespionage bis hin zu organisierter Kriminalität.

F&L: Sind vor allem forschungsstarke Universitäten betroffen?

Manfred Paul: Dazu kenne ich keine vergleichenden Zahlen. Aus dem, was wir mit den Rechenzentrumsleitern und Informationssicherheitsbauftragten erfahren, habe ich derzeit nicht den Eindruck.

F&L: Richten sich die Angriffe auf bestimmte Personen?

Manfred Paul: Der Großteil der Angriffe scheint eher ungerichtet zu sein. Sie sollen meist nicht mal konkret eine bestimmte Hochschule erreichen, sondern werden in großem Maßstab auch an andere Hochschulen, Unternehmen oder Privatpersonen verschickt. Sehr oft wird auch nur versucht, den Rechner zum Teil eines Bot-Netzes zu machen, damit werden sie Teil eines viel größeren Angriffsszenarios, das zur Gefahr für Universitäten wie auch staatliche Behörden oder Firmen werden kann. Große Botnetze können weltweit Millionen von Rechnern umfassen. Allerdings scheinen aber auch die gezielten Attacken auf Mitarbeiterinnen und Mitarbeiter einzelner Fachabteilungen zuzunehmen – auch in der Leitung. Das geht von dem direkten

Zusenden von Mail-Anhängen über den gezielten Angriff auf Schwachstellen von Servern bis hin zu sogenannten Social Engineering Angriffen wie zum Beispiel dem bekannten „CEO Fraud“, bei dem ein Mitarbeiter von einem angeblichen Leiter einer Organisation unter der Maßgabe von Geheimhaltung angewiesen wird, irgendwo hin Geld zu überweisen.

F&L: Wie erklären Sie sich die Zunahme gezielter Cyber-Angriffe?

Manfred Paul: Die Angriffsszenarios werden immer raffinierter, und wenn ein Angreifer bestimmte Daten haben möchte oder durch Ransomware eine Organisation lahmlegen möchte, sind gezielte Verbreitungswege wohl erfolgversprechender.

F&L: Wie können sich Hochschulen besser schützen?

Manfred Paul: Hochschulen müssen ihre potenzielle Angriffsfläche so weit wie möglich verkleinern. Dafür ist es ganz wichtig, dass sie die Anzahl der nach außen sichtbaren Systeme reduzieren, verschiedene Rollen und damit verbundene Rechte verteilen und die Zugriffsrechte soweit wie möglich einschränken. So haben Studierende an den meisten Hochschulen zum Beispiel bis auf Ausnahmen gar keinen Zugriff auf das interne Hochschulnetz, sondern können nur über das WLAN das Internet nutzen. Von der IT werden ihre Geräte als „nicht vertrauenswürdig“ eingestuft. Wir rechnen also schon damit, dass diese infiziert sein könnten, und blockieren den Zugriff auf interne Dienste so weit wie möglich. Auch bei den Beschäftigten werden die Gefahrenquellen so weit wie möglich eingeschränkt. Dozierende und speziell Forschende müssen aber teilweise Software installieren können, weil sie diese möglicherweise für Forschung und Lehre brauchen. Bei Beschäftigten in der Verwaltung und Rechnerräumen wird auch das unterbunden, genauso wie die Verwendung von USB Sticks, die damit vom System bewusst nicht erkannt werden, um eine mögliche Virenübertragung zu vermeiden.

F&L: Hochschulangehörige sind in der Cybersicherheit laut einer Studie kaum geschult. Was läuft schief?

Manfred Paul: Hochschulen verschicken bereits Informationsmails an alle Hochschulangehörigen und viele Studierende sowie Mitarbeiterinnen und Mitarbeiter melden sich auch, weil ihnen zum Beispiel verdächtige Mails auffallen. Aber wir müssen noch mehr tun. Das sehen wir zum Beispiel an vermeintlichen Phishing-Mails, die Hochschulen teilweise selbst als Übung für Studierende und Beschäftigte verschicken und die angeklickt werden. Sie sind eine hervorragende Möglichkeit, um Bewusstsein zu schaffen.

Klickt jemand auf den Anhang oder Links in dieser E-Mail erscheint ein Lernvideo, das erklärt, was hätte passieren können, wenn es sich dabei tatsächlich um eine Phishing-Mail gehandelt hätte und wie Hochschulangehörige künftig erkennen können, dass es eine solche ist. Wir brauchen noch mehr Schulungen zur Cybersicherheit, aber dafür fehlen uns Personal und Zeit.

F&L: Wie sind die Hochschulen aufgestellt?

> »Klassische Ansätze aus früheren Zeiten entsprechen nicht mehr dem Stand der Technik.«

Manfred Paul: Die meisten Hochschulen haben keine eigenen Budgets für Informationssicherheit, häufig erfolgt eine Querfinanzierung aus zentralen IT-Mitteln oder Fakultätsmitteln. Diese Summe ist jedoch aus Sicht der IT-Abteilungen zu klein, weil klassische Ansätze aus früheren Zeiten wie zum Beispiel einfache Firewalls und einfacher Virenschutz nicht mehr dem Stand der Technik entsprechen. Wir brauchen intelligente Technologien wie Next Generation Firewalls, bessere Möglichkeiten zum Monitoring unserer Infrastruktur oder KI-Konzepte für den Schutz von E-Mails und Endgeräten, aber auch größere Anstrengungen zur laufenden Sensibilisierung der Mitarbeiter. Im Rahmen der Digitalen Transformation, die auch vor Hochschulen nicht Halt macht, kommt der IT und deren Sicherheit eine steigende Bedeutung zu. Das heißt größerer Investitionsbedarf in Geräte und Personal. Informationssicherheit kostet Geld.

F&L: Wie viele Personen beschäftigen sich mit IT-Sicherheit?

Manfred Paul: Je nach Größe, Universitätstyp und Bundesland sind es zwischen 0,25 und einer Stelle für die Informationssicherheit an sich. Vom ZKI aus fordern wir mindestens 0,5 bis zwei Stellen pro Hochschule für die Rolle zentraler Informationssicherheitsbeauftragter, die dann aber noch auf Zuarbeit aus der Verwaltung und den Fakultäten angewiesen sind.

F&L: Eine halbe Stelle für die Cybersicherheit im gesamten Netz einer Hochschule?

Manfred Paul: Das Problem ist, dass nicht nur in der Politik das Bewusstsein für die Bedeutung solcher Stellen fehlt, dabei ist die Informationssicherheit ein wesentliches Kriterium für den Forschungsstandort Deutschland. Wir finden auch nur schwer gute Leute, weil ihnen in der Wirtschaft deutlich mehr Geld geboten wird. Das versuchen wir ein bischen abzufedern, indem wir uns untereinander noch besser vernetzen und Ressourcen bündeln.

F&L: Wie machen Sie das?

Manfred Paul: Das ZKI hat zusammen mit dem BSI im Rahmen der Allianz für Cybersicherheit ein „Grundschutzkonzept Hochschule“ erarbeitet, um gemeinsame Sicherheitsstandards festzulegen. Circa 60 Personen aus verschiedenen Hochschulen haben in regelmäßigen Workshops zusammengesessen und überlegt, wie die Netzwerke noch sicherer werden können. Zudem tauschen wir uns in Arbeitskreisen innerhalb der Bundesländer und über den ZKI regelmäßig über aktuelle Fragestellungen aus. Die Hochschulen sind weiter über das Deutsche Forschungsnetz (DFN) mit dem Internet verbunden, auch der DFN Verein stellt den Hochschulen zunehmend Dienstleistungen zur IT-Sicherheit zur Verfügung. Wir behelfen uns auf diese Art und Weise, bräuchten aber für die Umsetzung mehr Personal.

F&L: Können die Hochschulen von Glück sprechen, dass es noch nicht zu schwerwiegenderen Cyberangriffen gekommen ist?

Manfred Paul: Wir stellen uns im Rahmen unserer Möglichkeiten so gut wie möglich auf, aber ja, Glück hilft auch.

Die Fragen stellte Katrin Schmermund.