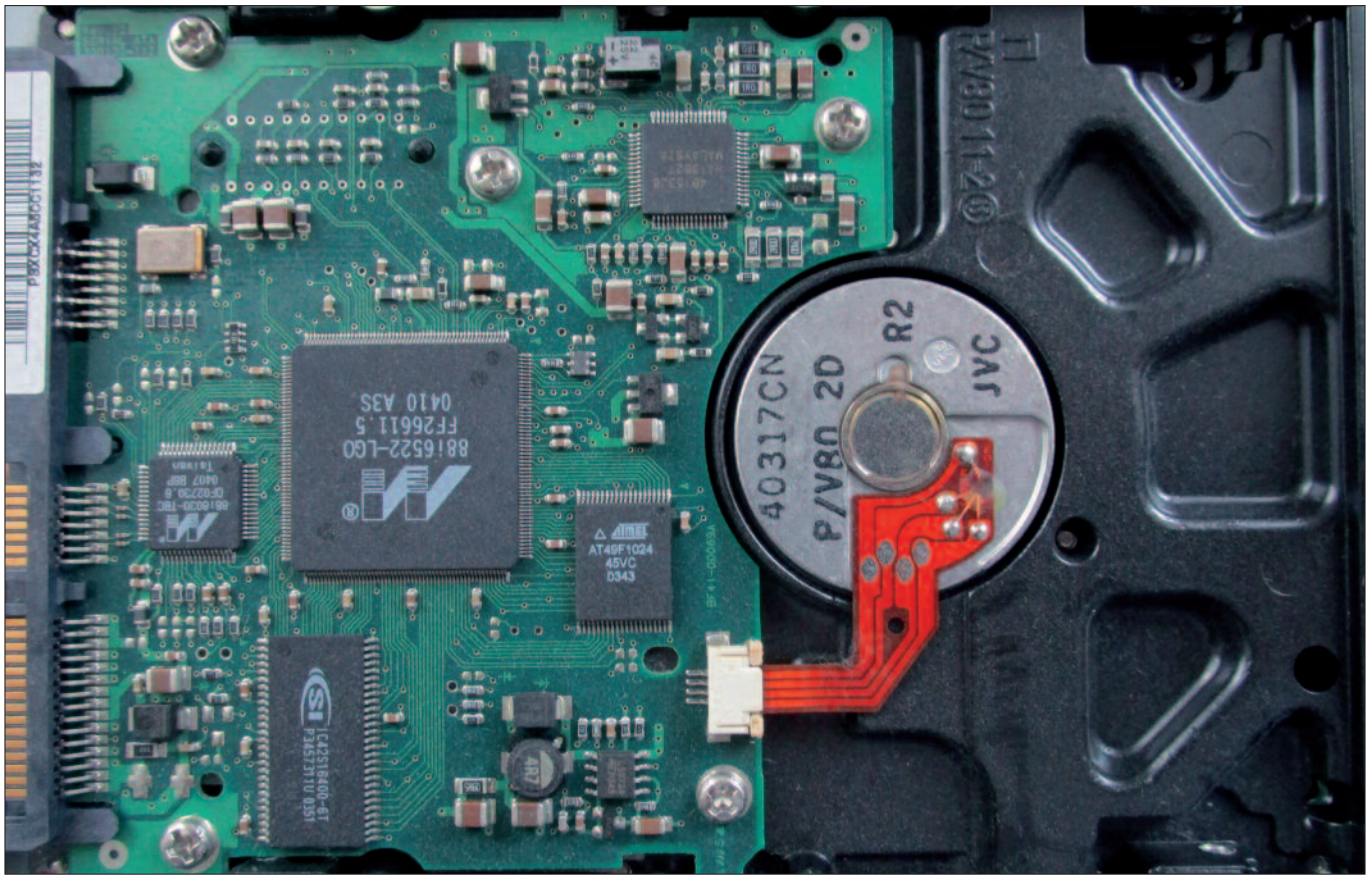


IT-Sicherheit: Vor Hackerangriffen schützen ein ganzheitliches Sicherheitskonzept, verbunden mit einem regelmäßigen Patch-Management und einem besonderen Schutz für Admin-Accounts. Nicht gebrauchte Software sollte entfernt werden.

Maßnahmen gegen Cyber-Angriffe

Auf dem Gebiet der IT-Sicherheit besteht weiterhin großer Handlungsbedarf. Das zeigte sich auch beim diesjährigen Security-Forum des Hagenberger Kreises.

Jeder könne ohne Nachweis einer Qualifikation als Programmierer arbeiten. Das sei eine der Ursachen, dass es in der IT-Welt zu Sicherheitsvorfällen komme, sagte DI Dr. Wolfgang Schwabl, CSO bei *A1,* beim *Security-Forum* des *Hagenberger Kreises,* das am 5. und 6. April 2017 in der Fachhochschule Hagenberg stattfand. Eine Berufsausbildung wie bei einem Arzt oder Elektriker sei nicht vorgeschrieben. Weiters würden, weil man das Rad nicht neu erfinden will, ältere Programme in neue Software eingebaut, ohne sie an geänderte Sicherheitsanforderungen anzupassen. „Keine Software ist fehlerfrei." Konflikte können sich ergeben, weil kein ausreichendes Testen erfolge. Andererseits blieben Testversionen am Rechner liegen und bildeten Einfallstore für Hacker. Funktionierende Systeme zu patchen, werde vielfach als Risiko angesehen und deshalb unterlassen. Das bezeichnete Schwabl als die „schlechteste Lösung": Entweder sollte man Patchen oder gleich neu installieren. Umstrukturierungen, das Auslagern von Dienstleistungen und Personalabbau hinterlassen in Unternehmen Wissenslücken über die Funktionsweise von Programmen, und letztlich sind Qualität, Verfügbarkeit und Sicherheit Kostenfaktoren.

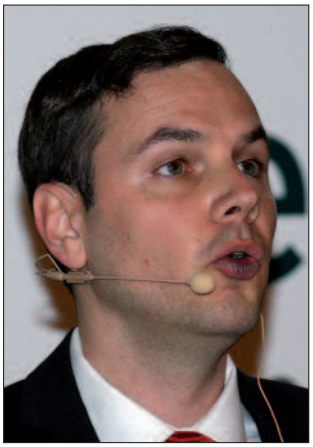
Bei entsprechender Aufmerksamkeit lassen sich Betrugsfälle verhindern: Die Niederlassung eines Unternehmens hätte einen auf über 30 Millionen Hongkong-Dollar (mehr als drei Millionen Euro) lautenden Betrag innerhalb weniger Tage überweisen sollen. Der Geschäftsvorgang war in der Mail, die angeblich vom CEO stammte, als streng vertraulich bezeichnet worden und wurde durch mitgelieferte Dokumente mit (gefälschter) Unterschrift des CEO belegt. Gesundes Misstrauen hat die Überweisung solange verzögert, bis der versuchte Betrug aufgeklärt werden konnte.

Eine per E-Mail versendete, verfälschte Rechnung wurde daran erkannt, dass – bei optisch gleichem Aussehen wie ein Original – eine andere, ungewöhnliche Bankverbindung angegeben war. Der Täter hatte sich zuvor eine dem (angeblichen) Rechnungsleger ähnliche Mailadresse zugelegt. Eine telefonische Rückfrage bei diesem hatte ergeben, dass die Rechnung nicht von ihm stammte.

Der angegebene Name des Absenders einer E-Mail kann falsch sein. Jemand anderer kann sich dahinter verstecken. Aus dem Briefkopf (Header) einer Mail (in Outlook abrufbar aus der Funktion Nachverfolgung und Drücken des Erweiterungspfeils unten rechts) kann rückverfolgt werden, von welchem Access-Provider die Mail gekommen ist.

FOTO: WERNER SABITZER

Kerstin Reisinger: „Systeme für die Gebäudeautomation haben Schwachstellen."



Thomas Brandstetter: „Schwache Passwörter ermöglichen Angriffe."

Wolfgang Schwabl: „Jeder kann ohne Ausbildung als Programmierer arbeiten."

Wolfgang Neudorfer: „Ganzheitliches Sicherheitskonzept erforderlich."

Wird man auf weiterführende Informationsmöglichkeiten verwiesen („Für weitere Informationen klicken Sie hier"), zeigt ein Drüberstreichen mit dem Mauszeiger, auf welche Website verwiesen würde. Warnungen vor Betrugsversuchen enthält die *Watchlist Internet (www.watchlist-internet.at)*. Die Rechtsgültigkeit elektronischer Signaturen und elektronischer Siegel kann über *https://www.signaturprüfung.gv.at* nachgeprüft werden. Von der Möglichkeit, Dokumente online mit der Handy-Signatur *(www.handy-signatur.at)* zu unterschreiben, machen immer mehr Nutzer Gebrauch. Mit Stand Ende Juli 2017 waren schon eine Million Menschen als Handy-Signatur UserInnen registriert, monatlich kommen etwa 20.000 dazu *(www.a-trust.at)*.

Insgesamt gilt es, die Cyber-Welt sicherer zu machen. Schwabl verwies in diesem Zusammenhang auf die von der *ENISA* ausgearbeiteten *Common Baseline Security Requirements,* die im Jänner 2017 veröffentlicht wurden und sich im Wesentlichen auf zehn Grundregeln stützen.

Gebäudeautomation. Ihren Ausgang hat die Gebäudeautomatisierung bei der Klimatechnik (Heizungsregelung, Jalousiensteuerung) genommen. In weiterer Folge sind Beleuchtung, Energietechnik (Waschmaschine, Fernseher), Transporttechnik (Aufzüge, Rolltreppen) und auch die Sicherheitstechnik hinzugekommen – alles über das Smartphone steuerbar. Die Systeme aber weisen Schwachstellen auf, die Thomas Brandstetter und Kerstin Reisinger, *Limes Security (www.limessecurity.com),* erläuterten. Die Technik der Hersteller hat mit der Entwicklung in der IT-Welt nicht mitgehalten. Es wird hinsichtlich der Sicherheit immer noch von in sich geschlossenen Systemen ausgegangen. Wenn Sensoren nicht authentifiziert sind, kann über einen solchen direkt auf das gesamte System zugegriffen werden. Ferner müsste die in elektronischen Geräten eingebettete Software *(Firmware)* upgedatet werden, um sie an neu entwickelte Angriffsszenarien anzupassen. Die Möglichkeit hiezu müsste von Haus aus vorgesehen werden, was kaum der Fall ist. In diesem Fall kämen Rückruf- oder Austauschaktionen in Frage, die eher selten sind.

Über die Suchmaschine Shodan können bestimmte Steuerungssysteme gefunden werden. Keine, ungeänderte oder schwache Passwörter ermöglichen dem Angreifer das Eindringen. Wenn dann auch noch die Mail-Adresse des Inhabers der Anlage im System hinterlegt ist, kann dieser persönlich angegriffen werden. Etwa dadurch, dass an einem kalten Wintertag die Heizung ausfällt, oder dass mitten in der Nacht in einem Gebäude falscher Feueralarm ausgelöst wird. Es könnte Lösegeld verlangt werden, damit der Spuk wieder aufhört. Auch Sicherheitseinrichtungen (Bewegungsmelder zur Beleuchtung, Videokameras zur Überwachung der Eingänge) könnten ausgeschaltet werden, um ungestört einbrechen zu können. „Der Computerwurm *Stuxnet,* der Industrieanlagen angegriffen hat, hat die Industrie wachgerüttelt", sagte Brandstetter. „Bei der Gebäudeautomation könnte Ähnliches noch bevorstehen."

Cyber-Angriffe. Die Vorgangsweise, wie *Red Teams* gegen *Blue Teams* antreten, schilderte Severin Winkler, *KPMG Cyber Security (www.kpmg.at)*. Das Red Team simuliert einen erfahrenen Angreifer auf die IT-Sicherheit des Blue Teams. Letzten Endes finden beide zu gemeinsamer Zusammenarbeit und Aufarbeitung in einem *Purple Team* zusammen. Entwickelt hat sich das *Red-Teaming* aus Penetrationstests *(Pentesting),* deren Ziel es ist, so viele Schwachstellen wie möglich zu finden, ohne dass allerdings „zu Ende gehackt" wird. Der Gegner wird zunächst ausgekundschaftet. Dann wird ein Schadcode implementiert, der sich im System festsetzt und danach trachtet, möglichst viele Zugriffsrechte zu erlangen *(Privilege Escalation)*. Mit diesen dringt er tiefer in das System ein und verbreitert sich auf der Suche nach den Assets *(Lateral Movement)*. Letztlich wird der Angreifer vom Blue-Team entdeckt und damit die Mission beendet.

Kriminelle Angriffe folgen von der Vorgangsweise her diesem Schema. Das stellte Wolfgang Neudorfer am Beispiel von *APT28* dar. Es handelt sich dabei um eine Gruppierung von Hackern, die sich auf Angriffe auf öffentliche Einrichtungen spezialisiert hat. Gemeinsam ist allen Gruppen, dass sie sehr gut organisiert und finanziell gut ausgestattet sind. Die Arbeitsweise gleicht der einem Unternehmen mit fixen Arbeits- und Geschäftszeiten. Das charakteristische Merkmal ist die Zielgerichtetheit ihrer Angriffe, die sehr lange, mitunter jahrelang, aufrechterhalten werden. Es geht um Geld und/oder vertrauliche Informationen. Am bekanntesten

FOTOS: KURT HICKISCH

sind die unter *Fancy Bear* und *Cosy Bear* auftretenden Kollektive geworden, die sich durch die von ihnen eingesetzte Malware-Familie und ihre Infrastruktur voneinander unterscheiden. Angriffsziele waren unter anderem die NATO, das ukrainische Militär und die Antidoping-Agentur.

Wenn sich der Angreifer schon über Monate hindurch eingenistet hat, kann man nichts anderes mehr machen, als die Systeme niederzufahren und neu aufzustellen, betonte Neudorfer. „Es gibt kein Silver Bullet." Vorbeugend hilft ein ganzheitliches Sicherheitskonzept, verbunden mit einem regelmäßigen Patch-Management und einem besonderen Schutz für Admin-Accounts. Nicht gebrauchte Software sollte entfernt werden.

Mitbewerber-Analyse. Es kann für ein Unternehmen von Interesse sein zu erfahren und nachzuprüfen, wie sicher seine Daten bei einem anderen Unternehmen abgelegt sind. Die Grenzen, die einem unautorisierten Penetrationstesting gesetzt sind, erläuterte Rechtsanwalt Dr. Lukas Fellner, *Baker&McKenzie (www.bakermckenzie.com)*. Industriespionage nach § 123 StGB liegt vor, wenn jemand ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben. Die nur auf Verlangen des Verletzten zu verfolgende Tat wird zu einem Offizialdelikt, wenn die Auskundschaftung zugunsten des Auslands erfolgt (§ 124 StGB).

Geschäftsgeheimnisse sind Tatsachen und Erkenntnisse kommerzieller oder technischer Art, die nur einer bestimmten und begrenzten Zahl von Personen bekannt sind, nicht über diesen Kreis hinausdringen sollen und an deren Geheimhaltung ein wirtschaftliches Interesse besteht. Der Geheimhaltungswille muss nicht ausdrücklich erklärt werden, sondern kann sich auch aus den Umständen ergeben, etwa durch einen Passwortschutz. Mangelhafte Sicherheitsstandards erlauben bei aufrechtem Passwortschutz nicht den Schluss, dass der Unternehmer kein Interesse an der Geheimhaltung mehr hätte (OGH 25.10.2016, 4 Ob 165/16t).

Fachhochschule Hagenberg in Oberösterreich: Jährliches „Security-Forum" des Hagenberger Kreises.

Nach § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) ist strafbar, sich zu einem Computersystem, über das der Täter nicht oder nicht allein verfügen darf, durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem Zugang zu verschaffen, wenn dies in der Absicht erfolgt, sich Kenntnis von schutzwürdigen personenbezogenen Daten zu verschaffen, oder einem anderen durch die Verwendung der gespeicherten Daten oder des Computersystems einen Nachteil zuzufügen. Die Tat wird mit Freiheitsstrafe bis zu 6 Monaten oder Geldstrafe bis zu 360 Tagessätzen bestraft. Wird die Tat in Bezug auf ein Computersystem der kritischen Infrastruktur oder im Rahmen einer kriminellen Vereinigung begangen, droht eine Freiheitsstrafe bis zu zwei Jahren; bis zu drei Jahren, wenn der Angriff auf ein Computersystem der kritischen Infrastruktur im Rahmen einer kriminellen Vereinigung erfolgt.

HAGENBERGER KREIS

Security-Forum

Alljährlich veranstaltet der Hagenberger Kreis an zwei Tagen im April das *Security-Forum* in der FH Hagenberg. Bei dieser Sicherheitskonferenz werden Probleme der IKT-Sicherheit aus technischer und juristischer Sicht behandelt. Das *Security-Forum* 2017 am 5. und 6. April 2017 hatte über 170 Teilnehmer. Die Vorträge wurden zum Teil in zwei parallel zueinander ablaufenden Panels abgehalten, teils in englischer Sprache. Der Hagenberger Kreis ist eine Vereinigung von Studenten und Absolventen der Studiengänge „Sichere Informationssysteme" (SIB – Bachelor, SIM – Master) an der Fachhochschule Hagenberg in Oberösterreich.

www.securityforum.at

Das „Herumprobieren", um das passende Passwort zu finden, ist zivilrechtlich eine Besitzstörung *(OGH 16.11.2012, 6 Ob 126/12s)*. Wird das Hacking über die IP-Adresse eines Unternehmens von einem Mitarbeiter durchgeführt, ist dieser als Gehilfe zur Besitzstörung anzusehen und es kann auf Unterlassung geklagt werden. Das Unternehmen wird schadenersatzpflichtig, wenn es sich wissentlich eines gefährlichen Mitarbeiters bedient (§ 1315 ABGB).

Technisch kann die Ausforschung des Access-Providers eines Täters über die *Whois*-Datenbank *(www.whois.com)* oder bei E-Mails über deren Header erfolgen. Auf Anordnung der Staatsanwaltschaft sind die Access-Provider zur Auskunft über Stamm- und Zugangsdaten des jeweiligen Teilnehmers verpflichtet (§ 76a StPO). Um dies zu erreichen, kann Strafanzeige gegen unbekannt eingebracht werden, gegebenenfalls (§ 118a StGB) zusammen mit der Erteilung der Ermächtigung zur Strafverfolgung. Bei einem Privatanklagedelikt (§ 123 StGB) scheidet diese Möglichkeit allerdings aus.

Bei Urheberrechtsverletzungen besteht ein vom Verschulden unabhängiger Anspruch des Rechtsinhabers auf Unterlassung (§ 81 UrhG), Beseitigung (§ 82 UrhG) und angemessenes Entgelt (§ 86 UrhG). Bei Verschulden kann vom Verletzten, wenn kein höherer Schaden nachgewiesen wird, das Doppelte des angemessenen Entgelts verlangt werden (§ 87 UrhG). Der Unternehmensinhaber haftet für das angemessene Entgelt, und zwar selbst dann, wenn er keine Kenntnis von der Urheberrechtsverletzung hatte, diese aber im Betrieb des Unternehmers begangen wurde. *Kurt Hickisch*

FOTO: KURT HICKISCH