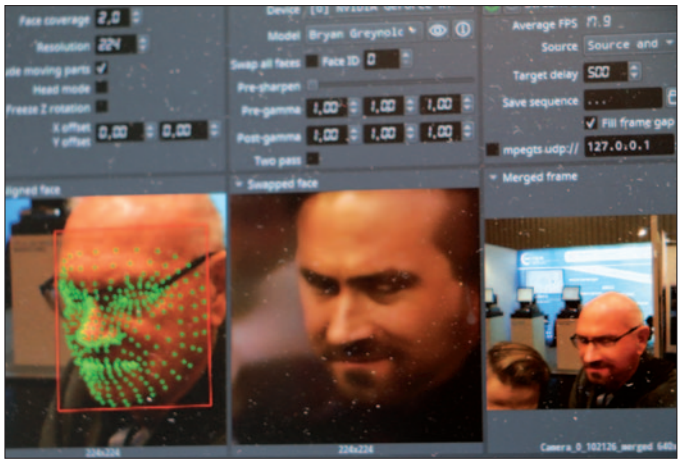

Generieren und Erkennen von Deepfakes

Sebastian Schreiber: Präsentation von Penetrationstests

Vorträge und Lösungen

Quantenkryptografie, Frauen in der IT-Sicherheitsindustrie, Hacking, Malware und Schutz kritischer Infrastruktur waren Themen der it-sa Expo&Congress Nürnberg, Europas führender IT-Fachmesse.

Die IT-Sicherheitsmesse *it-sa* fand vom 25. bis zum 27. Oktober 2022 im Messezentrum Nürnberg statt, begleitet von einem Kongress. Wenngleich technische Problemstellungen und -lösungen im Vordergrund standen, wurde etwa unter dem Titel „Women in Cybersecurity" erörtert, wie sich Frauen in die IT einbringen können und wie dem Fachkräftemangel begegnet werden kann. Auch Rechtsfragen wurden erörtert. In der Eröffnungs-Pressekonferenz bezeichnete Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern und Beauftragter der deutschen Bundesregierung für Informationstechnik, die Sicherheitslage im Cyber-Raum als mehr als angespannt, vor allem in der kritischen Infrastruktur. Er stellte notwendig werdende Änderungen des Grundgesetzes in Aussicht. Das *Bundesamt für Sicherheit in der Informationstechnik (BSI; bsi.bund.de)* soll dabei als Zentralstelle für Informationssicherheit eine umfassende, nicht mehr nur auf Nothilfe und auf Verwaltungsvereinbarungen beruhende Bundeskompetenz erhalten und bundesweit für die Gefahrenabwehr im Cyber-Raum zuständig werden.

BSI-Vizepräsident Dr. Gerhard Schabhüser stellte den Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2022 vor. Darin wird die Bedrohung im Cyber-Raum als so hoch wie noch nie bezeichnet. Bei Cybercrime bleibt die Cyber-Erpressung durch Ransomware besonders für Unternehmen die hauptsächliche Bedrohung. Allerdings wurden auch staatliche Stellen angegriffen. Bei einer Landkreisverwaltung in Sachsen-Anhalt waren bürgernahe Dienstleistungen über 207 Tage nicht verfügbar. Es wurde der Katastrophenfall ausgerufen.

Der russische Angriffskrieg auf die Ukraine zeigte sich laut Lagebericht bisher nur in Kollateralschäden, etwa bei Angriffen auf die Satelliten-Kommunikation. Als weiterer Schwachpunkt wurde die unzureichende Qualität der Software-Produkte bezeichnet.

Das BSI hat ein Grundschutzprofil für das 5-G-Mobilfunknetz sowie ein IT-Sicherheitskennzeichen vorgestellt, mit dem auf Antrag eines Herstellers Produkte gekennzeichnet werden, die die vom BSI anerkannten Sicherheitsanforderungen erfüllen. Der Link auf dem Siegel bzw. der QR-Code führen zu aktuellen Sicherheitsinformationen sowie zur Gültigkeitsdauer des Siegels. Mit der *Beschleunigten Sicherheitszertifizierung (BSZ)* werden Sicherheitsaussagen über ein IT-Produkt bestätigt. Seit 1. Oktober 2022 besteht auch die *Digitale Rettungskette* des Cyber-Sicherheitsnetzwerks.

Am Stand des BSI war ein Speakers Corner eingerichtet, an dem Vorträge unter anderem zur automatisierten Manipulation von medialen Identitäten (Deepfakes) oder zum digitalen Verbraucherschutz geboten wurden.

Mit einem Stand vertreten waren auch die *EU-Agentur für Cyber-Sicherheit (ENISA)* mit einem KMU-Leitfaden zur Cyber-Sicherheit sowie das Bayerische Landeskriminalamt, *Zentrale Anlaufstelle Cybercrime (ZAC)*. Das Cybercrime-Landeslagebild Bayern 2021 zeigt auch Möglichkeiten der Prävention auf.

OWASP. Das *Open Web Application Security Project (OWASP; owasp.org)* ist bekannt für seine Top Ten, eine Aufzählung der zehn häufigsten IT-Schwachstellen bei der Entwicklung von Anwendungen. Dabei handelt es sich nur um eines von derzeit 263 Projekten dieser globalen Non-Profit-Organisation, die, wie Tobias Glemser ausführte, die Verbesserung der Sicherheit von Software und Cyber-Sicherheit allgemein zum Ziel haben. Jeder, der daran interessiert ist, kann auf ehrenamtlicher Basis mitmachen. Die OWASP-Foundation gliedert sich weltweit in 233 lokale Chapters in 70 Ländern mit über 110.000 Mitgliedern.

Ein interessanter Gedankengang wurde von Johannes Klick, *Alpha Strike Labs (alphastrike.io),* vorgestellt. Das Unternehmen, ein Start-up, hat die Server- und Netzwerktätigkeiten in der Ukraine beobachtet und einen Zusammenhang mit russischen Angriffsoperationen festgestellt, die zu Schäden an der Infrastruktur geführt haben. Die Netzwerktätigkeit fiel im Angriffsgebiet bei solchen Operationen markant ab und erholte sich dann nur langsam. Im Zusammenhang mit anderen Berichten las-

Fotos: Kurt Hickisch

Start-up-Area auf der Fachmesse it-sa mit 16 Start-up-Unternehmen

sen sich auf diese Art Meldungen aus dem Kriegsgebiet objektiv verifizieren. Ein *Spillover-Effekt* (Auswirkungen auf andere Länder) oder ein *Cyber Pearl Harbor* konnten bis auf den bereits erwähnten Ausfall der Satellitenkommunikation nicht festgestellt werden.

Ethische Hacker spüren Schwachstellen in IT-Systemen auf, um die betroffenen Unternehmen zu warnen. Das niederländische Unternehmen *Intigriti (intigriti.com)* beschäftigt nach eigenen Angaben 50.000 ethische Hacker aus 140 Ländern. Diese werden mit einer „Bounty" (Spende, Kopfgeld) belohnt, wenn sie bei einem Vertragsunternehmen eine valide Sicherheitslücke entdeckt und dem Unternehmen gemeldet haben. Der Unterschied zu Penetrationstests besteht laut *Intigriti*, dass Bug-Bounty-Programme kontinuierlich ablaufen; die Bezahlung ergebnisorientiert erfolgt; ein kreativer statt ein technikorientierter Ansatz verfolgt wird und anstelle der Kompetenz und dem Fachwissen einzelner Experten das der Gemeinschaft zum Tragen kommt (Schwarmintelligenz).

Penetrationstests wurden von vielen Unternehmen angeboten. *Whitelisthackers (wlh.io)* steht in Verbindung mit der Challenge „Deutschlands bester Hacker" *(deutschlands-bester-hacker.de)*. Bereits 2020 war Frankens bester Hacker im Wettkampf ermittelt worden, 2021 jener von Bayern und 2022 Deutschlands bester Hacker. Als dieser wurde Leon, ein 17-jähriger Schüler, ermittelt und von Marco Di Filippo bei der *it-sa* vorgestellt. Die bei der Challenge gestellte Aufgabe hat darin bestanden, das fiktive *AKW Blackout* zu retten, von dem sensible Daten im Darknet veröffentlicht und von einer Untergrundorganisation bereits zu Geld gemacht wurden. Es bestehe die Gefahr eines Zugriffs auf die Steuerung der Kernreaktoren im Kraftwerk.

Die Qualifizierung für die Challenge 2023 beginnt am 5. Juli 2023. Es besteht keine Altersbeschränkung. Ziel des Wettbewerbs ist, das Hacking aus dem Dunkel zu holen und *White Hackers* zu fördern, um mit deren Hilfe die Sicherheit im Cyber-Raum zu erhöhen.

Sebastian Schreiber, *SySS GmbH (syss.de)*, führte in Live-Präsentationen vor, dass mit dem nötigen Fachwissen auch Krypto-Hardware geknackt oder eine Alarmanlage angegriffen werden kann. Auch Virenscanner können überlistet werden. Vorsicht bei Mails – sie müssen nicht unbedingt von dem stammen, der sich als Absender ausgibt.

Sobald Fonts (Schriftarten) auf die Website geladen werden, wird vom Anbieter die als personenbezogenes Datum geltende IP-Adresse erfasst, teilweise auch Browser- und Gerätedaten, und eine Verbindung zu den Servern des Anbieters hergestellt, wodurch es (Beispiel *Google*) zu einer Datenübermittlung etwa in die USA kommt. Nachdem sich daraus Abmahnverfahren als Geschäftsidee entwickelt haben, bietet das österreichische Unternehmen *Lukmann Consulting GmbH* mit dem „DSGVO-Website-Butler" *Alfright (alfright.eu)* die Analyse einer gesamten Website einschließlich aller Unterseiten auf Einhaltung der rechtlichen Bestimmungen wie DSGVO, BDSG, EU-Cookie-RL und TTDSG an. Bei diesem Auditing wird unter anderem überprüft, ob externe Dienste wie *Youtube* oder *Google Maps* ohne Einwilligung geladen werden, es Datenübertragungen in unsichere Drittländer gibt oder die Datenschutzerklärung (Art. 13 DSGVO) vollständig und noch aktuell ist. Gefundene externe Dienste, zu deren Nutzung keine Einwilligung erteilt wurde, die Datenübertragung nicht zulässig ist oder die Informationspflicht nicht erfüllt wurde, werden in einer Tabelle angezeigt. Das Unternehmen bietet des Weiteren Abmahnschutz und ein Datenschutzsiegel für die Website des Nutzers an.

Malware. Die *Deutsche Gesellschaft für Cybersicherheit (dgc.org)* definierte Malware als jegliche Software, die ohne

FOTO: KURT HICKISCH

FACHKONFERENZ

Personenschutz

In der Burg Deutschlandsberg in der Steiermark findet am 18. und 19. April 2023 die 3. Fachkonferenz *Personenschutz und Unternehmenssicherheit* statt. Zielgruppe sind Führungskräfte Personenschutz, Leiter Unternehmenssicherheit/Sicherheitsverantwortliche, Private Sicherheitsdienstleister/-Unternehmen. In der Konferenz geht es unter anderem um Digitales Alarm- und Notfallmanagement, Peter Endress (EVALARM Swiss Platinum Consulting); Unternehmenssicherheit im Großkonzern/Gefahren mit nationaler Filialenstruktur, Fabian Pfliegler REWE-Sicherheitsmanagement; IT im Unternehmen – Im Jahr 2023 immer noch ein Risikofaktor?/Angriffe aus dem Netz, Bernhard Otupal, Sicherheitsexperte beim IT-Unternehmen RISE; Die sieben W im Umgang mit Journalisten faktisch/praktisch, Michael Fleischhacker, Journalist; Wundbild und Erstversorgung bei Stich- und Schussverletzungen, Clemens Wissiak.

Anmeldeschluss: 22. Februar 2023; Information: www.closeprotection.at

Zustimmung des Opfers unerwünschte und schädliche Funktionen auf dem Computer ausführt. 75 Prozent der Malware werden nach dieser Darstellung über E-Mail und Phishing-Kampagnen eingeschleust. Um Identitäten zu imitieren, wird *Deepfake* und *Voice-Phishing (Vishing)* eingesetzt, letzteres auch durch Manipulation der Stimme einer Person *(Voice Swapping)*. Bei *Ransomware*-Angriffen würden 50 Prozent der kompromittierten Unternehmen Lösegeldzahlungen akzeptieren. Die durchschnittlichen wirtschaftlichen Auswirkungen pro Vorfall würden zwischen 1,73 und 3,7 Millionen Euro liegen. Im Durchschnitt werde erst nach 207 Tagen der Einbruch in das System erkannt, gefolgt von 73 Tagen, um den Betrieb erfolgreich wiederherzustellen.

Sicherheitslösungen. Die auf IT-Sicherheit ausgerichtete Messe bot einer derartigen Vielfalt von Ausstellern Gelegenheit, ihre aus den unterschiedlichsten technischen und strategischen Gesichtspunkten entwickelten IT-Sicherheitslösungen zu präsentieren, sodass im Einzelnen nicht diskriminierungsfrei darauf eingegangen werden kann. Es sollen im Weiteren, und auch hier wieder nur exemplarisch, Lösungen angeführt werden, die direkt beim Menschen, als dem schwächsten Glied der Kette, ansetzen. Immerhin beginnen, wie bei einem Kurzvortrag von *ThriveDX (thrivedx.com)* ausgeführt wurde, 95 Prozent der *Cyber Incidents* beim Mitarbeiter. Das Unternehmen bietet Cyber-Security-Awareness-Trainings an.

Laut *Hoxhunt (hoxhunt.com)* beginnen 93 Prozent aller Breaches mit einer Phishing-Email. Technologie biete nur zu 90 Prozent Sicherheit. Einige schädliche E-Mails würden immer in die Posteingänge der Mitarbeiter/-innen gelangen. Auch Hoxhunt setzt auf Phishing- und Awareness-Training, und zwar in einer Form von Gamification. Nach einer Einschulung werden Mitarbeitern in unregelmäßigen Zeitabständen Phishing-Mails geschickt, die es zu erkennen gilt – was entsprechende Bonifikationen zur Folge hat.

Keysight (keysight.com) setzt einen *Threat Simulator* ein, mit dem ein Selbsttest durchgeführt werden kann.

Proofpoint (proofpoint.com) überprüft in einem Insider-Threat-Management-System Verhaltensanomalien, um zu erkennen, ob vertrauliche oder kritische Daten aus einem Unternehmen

it-sa Expo&Congress 2022: Referenten Markus Richter, Jaya Baloo, Tobias Glemser und Marco di Filippo

nach außen gelangen (Data Loss Prevention).

Die *Fraunhofer FOKUS-Akademie (fokus-akademie.de)* stellt mit Hilfe von VR-Brillen eine virtuelle Umgebung zur Verfügung, in der Incidents, wie etwa auch ein Blackout, simuliert werden können.

IncreaseYourSkills (IncreaseYourSkills.com) befasst sich unter anderem mit der Generierung und dem Erkennen von *Deepfakes*.

Nach einer Untersuchung der Schweizer *Nevis Security AG (nevis.net)* haben Anwender bis zu 130 digitale Benutzerkonten und verbringen 12 Tage ihres Lebens damit, nach ihren Benutzernamen und Passwörtern zu suchen. 52 Prozent nutzen ein Passwort für mehrere Websites. 13 Prozent haben für alles nur ein Passwort, wobei Geburtstag oder Haustiernamen (21 %) oder Fantasiewörter mit Brute-Force-Attacken leicht zu knacken sind. Das Unternehmen bietet das Ersetzen von Passwörtern für alle Anwendungen durch biometrische Authentifizierung an. Der Passwort-Manager von *LastPass (lastpass.com)* lässt sich in bestehende Anwendungen integrieren, auch dann, wenn Mitarbeiter ihre Firmengeräte privat verwenden wollen.

Quantencomputing. Ein Höhepunkt der Messe war der Vortrag von Jaya Baloo, CISO von *Avast,* zum Thema Quantenkryptografie. Die in den Niederlanden lebende Forscherin berichtete über die Grundlagen des Quantencomputings und die, mit der enormen Rechenleistung des Quantencomputers einhergehenden Auswirkungen auf derzeitige kryptografische Verfahren. Derzeit werden in Rechnerfarmen Unmengen bisher nicht entschlüsselter Nachrichten bloß zu dem Zweck gesammelt, später entschlüsselt zu werden („capture now, decrypt later"). Public-key-Verfahren wie etwa RSA werden nicht mehr sicher sein. Dagegen ist Datenübermittlung über Quantenkanäle insofern abhörsicher, als jedes Dazwischentreten eines Dritten den quantenphysikalischen Zustand der Teilchen verändert und damit erkannt wird.

Die Sicherheit der Quantenkommunikation beruht nicht wie bisher auf Rechenoperationen, sondern ist physikalisch begründet. Europa dürfe, so Baloo, nicht nachlassen, seinen wissenschaftlichen Vorsprung auf dem Gebiet der Quantentechnologie zu halten. In der technischen Umsetzung seien Länder wie China bereits voraus.

Bei der it-sa Expo&Congress waren 693 Aussteller (2021: 273) aus 29 Ländern vertreten. Es wurden 15.229 Fachbesucher (2021:5.184) vor Ort gezählt. Weitere 1.848 waren während der Laufzeit der Messe auf der Online-Plattform *it-sa365* aktiv. Unter der Plattform *Congress@it-sa* fanden schon am Vortag der Messe eine Informationsveranstaltung der Firma *Cirosec GmbH* zu Trends in der IT-Sicherheit sowie messebegleitend die Jahrestagung der IT-Sicherheitsbeauftragten der Länder und Kommunen sowie weitere Firmenmeetings statt.

16 Start-up-Unternehmen hatten Gelegenheit, sich auf einer eigenen Fläche gemeinsam zu präsentieren. Auf fünf Foren (A – E) wurden während der Messetage rund 350 Fachvorträge geboten. Die Vorträge wurden aufgezeichnet und können über *it-sa365* im Internet abgerufen werden. Erforderlich ist, sich unter Angabe seiner Mail-Adresse und eines künftighin zum Einloggen verwendeten Passwortes kostenfrei als Nutzer anzumelden. Durch weitere Angaben zu Beruf, Unternehmen, Wirtschaftszweig wird man ein Teil der *it-sa* Community.

Die nächste *it-sa (it-sa.de)* wird vom 10. bis 12. Oktober 2023 wiederum im Messezentrum Nürnberg stattfinden.

Kurt Hickisch

Fotos: Kurt Hickisch