
**Ausstellungsstände beim 29. Symposium Sicherheit der Erste Group Bank AG in Wien**

# Sicherheit im Bankenwesen

**Von Cybercrime über Fake News bis zur Krisenbewältigung und Arbeitnehmerschutz spannte sich der Bogen der Themen des 29. Symposiums Sicherheit der Erste Group Bank AG.**

Themenschwerpunkte der Vorträge beim Symposium Sicherheit der *Erste Group* am 10. und 11. Oktober 2023 in Wien waren Informations- und physische Sicherheit, Datenschutz, Business-Continuity sowie Notfall- und Krisenmanagement und Arbeitnehmerschutz. Zielgruppe waren Sicherheitsverantwortliche von Geldinstituten und deren Umfeld.

**IT-Sicherheit.** „Der Markt für Cybercrime wird auf zweieinhalb Billionen US-Dollar geschätzt; Cybercrime wäre damit die drittgrößte Volkswirtschaft der Welt“, berichtete Joe Pichlmayr, *Ikarus Security Software (ikarussecurity.com),* über die „Erfolgsstory“ dieser Art von Kriminalität und deren dynamische Entwicklung. Pro Tag werden 80 Milliarden Ports auf Schwachstellen gescannt, 33 Millionen Phishing-Versuche unternommen und bis zu 300.000 (etwa 42 pro Minute) neue Malware-Programme entwickelt. Aus dem früheren Einzeltäter haben sich hochspezialisierte, global agierende Tätergruppen entwickelt. Der Grad der Vernetzung im *Internet of Things* steigt, ebenso die Zahl und die Komplexität der Angriffe, wogegen das Bewusstsein für die Bedrohungen und das Verständnis für das System sinken. Diese Entwicklung wird nur zum Teil durch Schulungen und Trainings abgefangen. Künstliche Intelligenz hat in der derzeitigen Entwicklungsstufe der schwachen KI nur eine begrenzte Lernfähigkeit. Eine starke KI, die sich an neue Situationen anpasst und sich selbst weiterentwickelt, liegt derzeit noch nicht vor. Das Problem ist der Mensch, der „Layer 8“ im siebenstufigen *OSI*-Modell für Netzwerkprotokolle. Bei der Projektstudie der Firma Ikarus *„klicken leute wirklich auf jeden link“* hatten vom 7. bis 14. Oktober 2008 3,37 Prozent der Besucher auf einen Link geklickt, der gefährlich hätte sein können. Eine Wiederholung des Tests zehn Jahre später brachte eine Klickrate von 5,4 Prozent. Computersysteme sollten ähnlich gesichert werden wie ein Haus gegen Einbrüche, mit Außen- und Innensicherung, weiteren präventiven Maßnahmen wie richtiges Verhalten und Beitrag zur Schadensminimierung. Einbrüche sind eher selten, bergen für den Täter ein hohes Risiko, er hat nur wenig Zeit. Der Schaden wird sofort bemerkt, Folgeschäden sind absehbar. Der Hacker kann zahllose Angriffe starten, geht nur ein minimales Risiko ein und hat jede Menge Zeit. Er bleibt lange unbemerkt, Folgeschäden sind kaum abschätzbar. Das „Diebsgut“ besteht aus Informationen und Identitäten. Anders als beim Einbrecher besteht eine hohe Wahrscheinlichkeit neuer Angriffe.

**Fake News.** „Internet und Social Media haben eine neue Form der Kommunikation geschaffen“, führte Andre Wolf von *Mimikama, Verein zur Aufklärung über Internetmissbrauch (mimikama.at),* aus. Aus einem Konsumenten von Nachrichten, die von einigen wenigen Sendern geprüft ausgegangen sind und wenig oder späte Resonanz hatten, wurde der Prod-User, der selbst Nachrichten versendet, kaum gefiltert. Noch nie hatte die Gesellschaft so schnell Zugang zu so vielen Informationen, bei denen sich Fakten, Meinung, Satire, Unterhaltung und Desinformation vermischen. KI kommt als neue, schwer einschätzbare Variable dazu. Der Prod-User kann manipulieren, aber auch selbst manipuliert werden.

Fake News beginnen dort, wo gezielte Desinformation betrieben wird. Darunter fallen nicht handwerkliche journalistische Fehler wie Headlines und Teaser so zu gestalten, dass sie mehr versprechen, als der Inhalt hergibt, um den Leser anzulocken und zum „Klicken“ zu animieren oder die „Zeitungsente“, eine versehentlich falsche Meldung. Die Desinformation kann sich äußern als bewusst falsche Interpretation wahrer Informationen, Manipulation wahrer Informationen, wie etwa von Bildern oder durch erfundene Inhalte.

Manipulierter Inhalt bei Bildern kann durch eine Rückwärtssuche erkannt werden. Die älteste Version eines Bildes ist am ehesten das Original. Bilder können in Suchmaschinen wie *Tin-Eye (tineye.com)* hochgeladen werden. Auch bei *Google-Lens* (er-

FOTOS: KURT HICKISCH

**Referenten Christian Wehrschütz, Elisabeth Daniel, Eckhard Jann, Ingrid Luttenberger, Natascha Smertnig, Joe Pichlmayer**

kenntlich am Kamera-Symbol beim Aufrufen der Website). Zur Bildersuche kann *Bing* verwendet werden oder die Suchmaschine des niederländisch-russischen Unternehmens *Yandex*. Beim Hochladen von Bildern in die Suchfunktionen der Bildagenturen *Shutterstock* oder *Adobe Stock (stock.adobe.com)* werden auch ähnliche Bilder ausgeworfen.

Mit KI generierte Bilder können insofern erkannt werden, dass sie Eigenheiten bei der Darstellung von Menschen aufweisen, etwa Fehler in der Anatomie oder fehlender Symmetrie bei Gesichtsbildern. Bilder wirken zu glatt und wenig lebensnah. Manche Darstellungen enden im Nichts. Vorgaben bei der Erstellung der Fakes wie etwa die Wiedergabe von Stimmungen oder für Hintergründe ziehen sich durch das gesamte Bild. Schriftzüge erscheinen verschwommen – die KI ist nicht auf Buchstaben trainiert.

„Wichtig ist zu wissen, wonach man überhaupt sucht, etwa die älteste Fundstelle, Originalgröße und -kontext, oder ähnliche Bilder“, betonte Wolf. Dazu gehört, die Quellen (Pressemedien, Urheber samt dessen URL, Meta-Daten der Bilder) zu überprüfen. Wird über dramatische, von KI generierte Situationen auch in anderen Quellen berichtet?

Bei Fake News liegt das Problem in deren massenhafter Verbreitung und in den Zusammenhängen (Narrativen), die damit verbunden werden und die Darstellung glaubhaft erscheinen lassen. Dabei kommt der *Confirmation Bias* (Bestätigungsverzerrung) ins Spiel, eine Voreingenommenheit, dass man geneigt ist, nur zu glauben, was man schon weiß. Seit 2014, dem Beginn der Krimkrise, werden die Social Media mit hochpolitischen Inhalten und manipulativen Narrativen überflutet. Zum „Beweis“ werden insbesondere von „alternativen Medien“ häufig Falschmeldungen verbreitet. Diese Medien können dazu neigen, Verschwörungstheorien zu fördern.

Der ORF-Reporter Christian Wehrschütz berichtete, unter anderem am Beispiel des am 17. Juli 2014 über der Ost-Ukraine abgeschossenen Passagierflugzeugs Flug MH17 der *Malaysian Airlines*, über die Schwierigkeiten, den Wahrheitsgehalt von Informationen zu ermitteln. Wehrschütz hatte damals am Absturzort recherchiert. Bei polarisierenden Themen entwickle sich ein Glaubenskrieg, und es werde immer Menschen geben, die man nicht überzeugen könne. „Keine Lüge kann so groß sein, dass sie nicht geglaubt wird“, meinte Wehrschütz und, dass Journalisten oft die ersten Opfer von Fake News seien. Wenn eine Nachricht viral gehe, sei sie kaum noch zu stoppen.

**Prävention im Bankenbereich.** Einen Einblick, wie die *Erste Bank und Sparkassen* sich und Kunden vor Betrug schützen, gaben Kristina Eder und Stefanie Trapp. Betrug kann aus dem Zahlungsverkehr entstehen, sich bei Kreditanträgen ergeben oder bei der Verwendung von Kreditkarten. Auf Betrugsszenarien im Internet wird in der *Watchlist Internet (watchlist-internet.at)* hingewiesen. Derzeit etwa, dass bei Second-Hand-Verkäufen im Internet vermeintliche Käufer auf gefälschte Zahlungsplattformen locken. Gewarnt wird auch vor Anrufen angeblicher Bankmitarbeiter *(Call-ID-Spoofing)*.

Elisabeth Daniel, *Erste Group*, berichtete über ein Security-Awareness-Programm, bei dem neue Wege zur Hebung des IT-Sicherheitsbewusstseins beschritten werden. Im Oktober 2023 wurde beim *Europäischen Cyber-Security-Month (ECSM)* der *ENISA* das Brettspiel *Bankers vs. Hackers* vorgestellt. Ferner wurden zusammen mit einer Marketingfirma kurze Videos produziert, die Themen der IT-Sicherheit einfach erklären. Als Belohnung werden Goodies angeboten.

Mitunter gilt es, Mitarbeiter vor psychischer oder körperlicher Gewalt zu schützen. Dem Freundlichkeitsdruck im Dienstleistungsbereich steht, wie Ingrid Luttenberger ausführte, eine zunehmende Aggressivität und Respektlosigkeit durch Kunden gegenüber. Der Arbeitgeber hat aus Gesichtspunkten des Arbeitnehmerschutzes entsprechende Maßnahmen technischer, organisatorischer und personeller Art zu treffen, damit aus einem bestehenden Risiko keine Gefahr wird.

**Fehlerkultur.** Eckhard Jann, Pilot sowie Berater und Experte für Fehlerkultur *(safetyone.de)*, zeigte anhand von Unfallstatistiken auf, wie sehr die Luftfahrt aus Fehlern gelernt hat, bis man zu dem derzeit hohen Sicherheitsstandard gelangt ist. In allgemeiner Betrachtung entstehen aus 15.000 beobachtbaren Arbeitsfehlern 300 Vorfälle und leichte Unfälle, 15 schwere Vorfälle und ein gravierender bis tödlicher Unfall (Heinrich-Pyramide). Fehlerketten müssen erkannt und möglichst früh unterbrochen werden. Eine von Angst freie Unternehmensorganisation und ein nicht punitives Meldesystem ermöglichen ein Aufarbeiten von Vorfällen, wobei ein kontinuierlicher Verbesserungsprozess im PDCA-Zyklus *(Plan-Do-Check-Act)* einzuhalten wäre.

Erfahrungen sollte man mit anderen teilen, weil man, so ein zitiertes Bonmot des Flugpioniers William Wright, nicht lange genug lebt, um alle Fehler selbst zu machen.

**Krisenbewältigung.** Als Erfolgsfaktoren zur kommunikativen Bewältigung einer Krise bezeichnete Lisa Sophie Grohs, *Wien Energie*, am Bei-

FOTOS: KURT HICKISCH

spiel einer im Unternehmen plötzlich eingetretenen Krisensituation, Prävention, Geschwindigkeit und Kontinuität. Prävention erfordert Vorbereitung und Planung. Strategien und Strukturen sowie Entscheidungswege und Prozesse sind vorab festzulegen. Etablierte Kanäle und reichweitenstarke Social-Media-Kanäle sind ein Startvorteil ebenso wie ein eingespieltes Team und grundsätzliche Expertise in Krisenkommunikation.

Geschwindigkeit in der Kommunikation, vor allem als Reaktion auf Social Media, verhindert, dass Dritte die Geschichte als Erste erzählen. Erste interne Informationen müssen an Führungskräfte ergehen. In weiterer Folge sind Sprachregelungen und Basis-Schreiben an Kunden, Lieferanten, erforderlich. Es muss Mut zu Pro-Aktivität aufgebracht werden. Kontinuität bedeutet tägliche Presseinformation mit Updates, laufende Information auf Social Media, Aufbereitung von Faktenchecks, Hintergrundinformationen, Richtigstellung von Falschmeldungen und aktive Kontaktaufnahme mit Schlüsseljournalisten. Informieren, wiederholen, durchhalten, sind in dieser Phase die Erfolgsfaktoren.

**Datenschutz.** Gregor König, Erste Group, berichtete über Entwicklungen auf dem Gebiet des Datenschutzes. Nachdem es für die Übermittlung von personenbezogenen Daten in die USA bereits zwei Angemessenheitsbeschlüsse der EU-Kommission gegeben hatte *(Safe Harbor und Privacy Shield)*, die beide vom EuGH aufgehoben wurden (Urteile *Schrems I* und *Schrems II*), liegt nunmehr, auf der Basis des *Data Privacy Frameworks*, ein neuer Angemessenheitsbeschluss der EU-Kommission vor, sodass die USA datenschutzrechtlich als sicherer Drittstaat zu betrachten sind. Hinsichtlich des *Artificial Intelligence Act* der EU hat das Parlament zwischenzeitig, am 9. Dezember 2023, eine vorläufige Einigung mit dem Rat erzielt. Die offizielle Annahme steht noch aus.

Auf Grund einer bei der irischen Datenschutzbehörde eingebrachten Klage des von Max Schrems gegründeten *Europäischen Zentrums für digitale Rechte (NOYB; noyb.eu)* wurden erstinstanzlich gegen *Meta* (Dienste wie *facebook* und *Instagram*) Rekordstrafen von Hunderten Millionen Euro verhängt. In Entsprechung der Whistleblowing-RL (EU) 2019/1937 ist nach kurzer Übergangsfrist am 25. Februar 2023 das HinweisgeberInnenschutzgesetz – HSchG, BGBl I Nr. 6/2023, in Kraft getreten.


**Ausstellungsstand: Sicherheitsprodukte und -dienstleistungen**

**Verbrechensopferhilfe.** Im Zentrum der Tätigkeit des seit 1978 bestehenden Vereins *WEISSER RING (weisser-ring.at)* stehen, wie Geschäftsführerin Natascha Smertnig, ausführte, alle Opfer von Straftaten mit ihren Bedürfnissen und Interessen, ohne dass unterschieden wird nach Alter, Geschlecht, ethnischer Zugehörigkeit, religiöser, politischer oder sexueller Orientierung. Schwerpunkt sind die Opfer situativer Gewalt wie Opfer von Internetkriminalität (Hass im Netz, Betrugsdelikte), Opfer von Hasskriminalität, von Gewalt am Arbeitsplatz (besonders betroffen Beschäftigte in Dienstleistung, Handel, Verkehr, Gesundheit) oder betagte Opfer von Straftaten, insbesondere bei Diebstahl und Betrug.

Auswirkungen von Gewalt können sich körperlich äußern (Herzrasen, Zittern, Krämpfe Übelkeit, Inkontinenz; Folgeschäden), psychisch (Angst, Panikattacken, Wut und Aggression, Trauer, Gefühl der Machtlosigkeit und Verlust des Sicherheitsgefühls, Selbstvorwürfe) und in sozialer Hinsicht (finanzieller Verlust, Probleme in der Arbeit bis zum Verlust des Arbeitsplatzes; Schwierigkeiten, in das soziale Leben zurückzufinden; Kosten für Sicherheitsmaßnahmen, medizinische Behandlung und Psychotherapie). Verbrechensopfer brauchen aber nicht nur Hilfe und Schutz, sondern haben auch Rechte nach dem Verbrechensopfergesetz (VOG). Erforderlich ist ein Antrag beim Sozialministerium. Die Straftat, die zu einer Körperverletzung, Gesundheitsschädigung oder gleichwertigen psychischen Verletzung geführt hat, muss mit einer Freiheitsstraße von mehr als sechs Monaten bedroht sein. Verbrechensopfer haben nach den §§ 66b und 65 StPO Anspruch auf Prozessbegleitung im Gerichtsverfahren, nicht allerdings bei Vermögens- und Eigentumsdelikten. Der WEISSE RING ist die einzige, gesetzlich anerkannte, allgemeine Opferunterstützungs-Einrichtung Österreichs (§ 14c VOG). 2022 betreute der Verein 1.824 Klienten in der Opferhilfe (52 % Frauen, 48 % Männer). 67 Fälle betrafen Gewalt am Arbeitsplatz. Die Website wurde 85.237-mal aufgerufen.

Im Foyer waren Aussteller von Sicherheitsprodukten und -dienstleistungen vertreten. Auf Interesse stieß das Security-Awareness-Training von *Hoxhunt (hoxhunt.com)*: Das Unternehmen versendet automatisiert an die Mitarbeiter seiner Kunden jährlich Dutzende gezielte, unterschiedliche Phishing-Simulationsmails. Werden diese richtig erkannt, rückt der Mitarbeiter in einen höheren Level auf, andernfalls fällt er wieder zurück. Parallel dazu stellt das Unternehmen Reports über die aktuelle Bedrohungslage zur Verfügung.

Das *30. Symposium Sicherheit* wird am 8. und 9. Oktober 2024 wieder in Wien stattfinden. *Kurt Hickisch*

Fotos: Kurt Hickisch