Cyberkriminalität und Risiken in der „digitalen Sphäre“

Aktuelle und zukünftige Bedrohungslagen sowie tragfähige Präventionsmaßnahmen

Von Dr. Viktoria Schäfer und Dr. Yvonne Zimmermann, Montabaur[1]

1 Inhalte und Kontext des Beitrags

Der vorliegende Beitrag befasst sich mit dem Thema Cyberkriminalität und geeigneten Präventionsstrategien. Im Hinblick auf die Prävention werden in Unternehmen und anderen Organisationen mittlerweile entsprechende Schulungen von Mitarbeitern entwickelt und gezielte Weiterbildungsangebote umgesetzt. Solche Maßnahmen bilden einen wesentlichen inhaltlichen Gesichtspunkt des Beitrags, der insbesondere an Schwerpunktthemen der Ausgabe 2/2022 der Zeitschrift Die Kriminalpolizei anknüpft. In dieser Ausgabe wurden Herausforderungen der Cyberkriminologie ausführlich erläutert. Handlungsleitend ist demnach die Erkenntnis, dass bei der Digitalisierung nicht primär an die Nutzung technischer Möglichkeiten und Geräte gedacht werden sollte, sondern an die „Etablierung eines globalen digitalen Raumes – besser vermutlich einer globalen digitalen Sphäre – der grenzfreien Interaktion und Kommunikation zwischen Menschen auf der ganzen Welt und aus jedem Kulturkreis“.[2] Die Folgerung, dass die Komplexität dieser digitalen Sphäre mit den sich hierin stellenden Deliktsmöglichkeiten der Entwicklung einer zukunftstragenden Polizeistrategie bedarf, ist vollauf nachvollziehbar. Der für eine solche Polizeistrategie relevante Präventionsgedanke wurde in der oben genannten Ausgabe auch in einem Fachartikel zur Sensibilisierung für Gefahren im Netz und zur Bekämpfung der verschiedenen Formen der Computerkriminalität unter besonderer Berücksichtigung der Schutzbelange von Kindern und Jugendlichen vertieft.[3] Erläutert wurden in weiteren Fachartikeln ferner Entwicklungen, Begehungsformen sowie Präventionserfordernisse und strafrechtliche Anforderungen im Deliktfeld „Identitätsdiebstahl und -missbrauch im Internet“.[4]

2 Präventionsorientierung möglichst früh vollziehen

Die Notwendigkeit der Präventionsorientierung in der digitalen Sphäre wurde unter dem forensischen und strafrechtlichen Blickwinkel in den angeführten Fachartikeln ausdrücklich hervorgehoben. Faktisch ist (leider) davon auszugehen, dass die Ausprägung und Deliktsrelevanz der verschiedenen Facetten der Cyberkriminalität auch zukünftig zunehmen werden. In Forschung und Praxis herrscht Konsens dahingehend, dass man solch einer problematischen Entwicklung durch eine möglichst früh, also bereits in der Schule erfolgende Verankerung von Präventions- und Abwehrstrategien begegnen sollte. Ein aktuelles Beispiel dafür ist „ChatScouts“, ein Projekt des LKA Niedersachsen. Dieses in Kooperation mit den Regionalen Landesämtern für Schule und Bildung (RLSB) und der Zentralstelle Jugendsachen des Landeskriminalamtes (LKA) Niedersachsen entwickelte Projekt erfuhr überdies die Unterstützung der kriminologischen Forschungsstelle des LKA Niedersachsen und spezialisierter Kräfte der Polizei Niedersachsen. Als Präventionsangebot richtet es sich an Kinder und verfolgt unter anderem das Ziel, Themen wie Cybermobbing und Mediensicherheit altersgerecht aufzubereiten. Hierzu werden neben Informationen, Unterrichtsmaterialien sowie Empfehlungen für pädagogische und polizeiliche Fachkräfte altersentsprechende Videoinhalte für die Kinder bereitgestellt. In seiner Gesamtheit beinhaltet das Projekt über die für Kinder entwickelten Elemente hinaus auch Empfehlungen für pädagogische Fachkräfte sowie, begleitend zu den Präventionsangeboten der Polizei an Schulen, Maßnahmen zur Einbeziehung und Sensibilisierung der Elternschaft.[5]

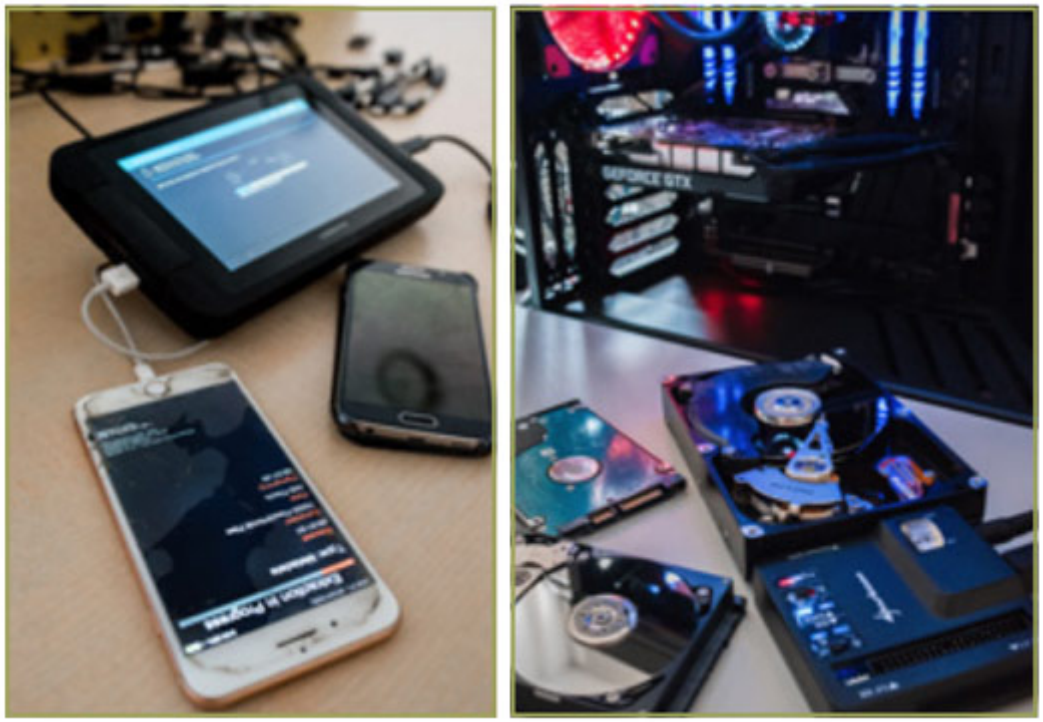
3 Transfer der Präventionsausrichtung auf den Berufsalltag – Bedrohungslage für KRITIS

Das LKA-Projektbeispiel zeigt einen Weg, wie die möglichst frühzeitige Aufklärung über Risiken in der digitalen Sphäre und die Vermittlung eines verantwortungsvollen Umgangs mit digitalen Medien realisiert werden kann. Solch eine – sinnvollerweise kontinuierlich angelegte – Präventionsarbeit kann entscheidend dazu beitragen, dass die Bewusstseinsbildung für die genannten Risiken und die erforderliche Verantwortungsherausbildung auch über die weitere Lebensspanne erfolgen und dann im Erwachsenenalter bzw. bei der Berufsausübung in Organisationen, Unternehmen usw. wirksam werden. Letzteres Ziel ist umso wichtiger, da – neben den die Betroffenen oftmals psychisch schwer belastenden „Individualattacken“ von Cyberkriminellen (wie etwa Identitätsdiebstahl im Internet, Cybermobbing oder Cyberstalking)[6] – die gegen Unternehmen, Behörden und andere öffentliche Einrichtungen ausgeübte Cyberkriminalität immer mehr zunimmt. Man spricht in diesem Zusammenhang auch von „Big Game Hunting“, also von Cyberattacken auf herausragende Wirtschaftsunternehmen sowie Einrichtungen der sog. Kritischen Infrastrukturen (KRITIS). KRITIS repräsentieren „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“.[7] KRITIS finden sich insbesondere in Bereichen wie der Energie- und Wasserversorgung, der medizinischen Versorgung und des öffentlichen Verkehrs. Fakt ist, dass in jüngster Zeit KRITIS, zu denen neben der Versorgung der Bevölkerung mit wichtigen Leistungen auch Verwaltungen mit großen Mengen an gespeicherten persönlichen Daten gehören, immer stärker in den Fokus von Cyberkriminellen geraten. Laut Expertenmeinung hat sich diese Situation seit dem Einmarsch russischer Streitkräfte in die Ukraine verschärft: „Gerade der Ukraine-Konflikt hat hier eine neue Komponente noch einmal in Erinnerung gerufen: Angriffe auf die Netzwerke öffentlicher Verwaltungen tragen dazu bei, einen Staat und eine Regierung massiv zu destabilisieren und das Vertrauen von Menschen in den Staat zu schwächen“.[8]

4 Hybride Konfliktaustragung und Cyberattacken, Angriffsformen und Schäden

Tatsächlich hat der Krieg in der Ukraine noch einmal mit Nachdruck auf die Gefahr der sog. hybriden Kriegsführung aufmerksam gemacht, denn kriegerische Auseinandersetzungen und geopolitische Konflikte können sowohl physisch mit Waffen als auch auf digitalen Ebenen ausgetragen werden: „Der Krieg zwischen Russland und der Ukraine erreicht durch die Anwendung der hybriden Kriegsführung eine neue Stufe der Bedrohung. Es werden nicht nur konventionelle, sondern zunehmend auch Cyberwaffen eingesetzt, um Regierungs-, Infrastruktur- und Energie- sowie private Netzwerke zu zerstören. In der Ukraine begann dieser ‚stille‘ Krieg bereits Stunden vor dem Einmarsch der russischen Truppen, um die Kommunikation zu erschweren bzw. zu unterbrechen. Darüber hinaus sollen dadurch Panik geschürt, Falschinformationen verbreitet und das Vertrauen sowie die Moral der Bürger zur Verteidigung untergraben […] werden“.[9] Im Zuge solcher Entwicklungen rücken die Cybersicherheit und damit Anstrengungen zur Verteidigung eines Landes, seiner Wirtschaft, Infrastruktur und letztlich der gesamten Gesellschaft gegen externe Cyberangriffe nochmals stärker in den Mittelpunkt. Datenauswertungen auf Basis aktueller Untersuchungen des Instituts der Deutschen Wirtschaft (IW) belegen für den Zeitraum von 2011 bis zur Gegenwart, dass schwere Cyberattacken auf Ziele in Deutschland[10] in 28% solcher Fälle ihren Ursprung in Russland hatten. Chinesische und iranische Akteure waren gemäß den Daten für 12% und 8% der Fälle verantwortlich. Es gilt aber auch kritisch darauf hinzuweisen, dass für weitere 4% dieser Fälle ein Ursprung in den USA identifiziert werden konnte und sich 48% der

schwerwiegenden Attacken seit 2011 nicht eindeutig einem Staat zuordnen ließen.[11]
Der Gesamtschaden durch Cyberangriffe ist sehr hoch. Bereits 2020, im Jahr des Ausbruchs der Corona-Pandemie, entstanden der deutschen Wirtschaft durch diese Angriffe, verbunden mit dem Diebstahl von Daten, Spionage sowie Sabotage, Schäden von schätzungsweise rund 224 Mrd. Euro[12] Der durch die Pandemie ausgelöste Digitalisierungsschub hat die digitale Gefährdungslage offenkundig verschärft. Im Rahmen dieses Digitalisierungsschubes haben auch die industrielle Vernetzung und Steuerung sowie das damit verknüpfte „Internet of things" (IOT) ausgeprägte Innovationsimpulse erfahren. Intelligente Steuerung macht Fertigungsprozesse effizienter, die sog. „smarte Analytik" trägt durch vorausschauende Wartung zur Verhinderung des Ausfalls von Anlagen bei und maschinelles Lernen in der Fertigungskontrolle hebt die Qualität von Waren und Produkten. Die entsprechenden Leistungen im Maschinenbau, der Automatisierungstechnik und im zugehörigen Software-Engineering sind beeindruckend, sollten jedoch nicht den kritischen Blick auf potenzielle Gefahrenquellen trüben, denn „das Risiko von Cyberattacken [wird] im Zuge der Vernetzung kontinuierlich immer größer. Mit jeder weiteren Maschine, jedem neuen Sensor, jedem zusätzlichen Gerät, das via Intra- und Internet auswert- und erreichbar wird, wächst die Gefahr, dass diese industriellen Steuerungssysteme auch zum Ziel von Hackerattacken werden".[13] Experten sprechen diesbezüglich von „OT-Attacken" durch Cyberkriminelle oder im Auftrag von Fremdstaaten handelnden Hackern (OT steht für operationale Technik).



Mobil- und Datenträgerforensik

OT-Angriffe und die weiter vorn angesprochenen Attacken auf KRITIS weisen teils Überschneidungsbereiche auf, die destruktive OT-Stoßrichtung zielt allerdings auf Unternehmen unterschiedlicher Branchen und Größenordnungen, also auch auf sog. KMU (kleinere Firmen und Mittelständler). Die zielgerichteten OT-Angriffe erreichen noch nicht das Ausmaß herkömmlicher IT-Attacken, die schon längst ein „digitales Trommelfeuer" auf die Firewalls und Virenschutz-Programme von Unternehmen darstellen, werden aber nach Prognosen von Fachleuten drastisch zunehmen und bergen enorme Schädigungsrisiken. OT-Angriffe zielen auf computergesteuerte Produktions- und Steuerungsanlagen, auf entsprechende Produktionsmaschinen und Fertigungstechnik sowie auf die Hard- und Software, die Geräte, Anlagen und Prozesse in industriellen Umgebungen steuert bzw. überwacht. Die Schädigungsrisiken können sich auf Leib und Leben erstrecken: „das Schadensrisiko reicht weit über den bloßen Stillstand von IT-Systemen hinaus: Denn OT-Attacken können von reinen Maschinenstörungen und Fehlfunktionen bis hin zur kompletten mechanischen Zerstörung der Technik führen. Dass dabei, etwa beim Bersten von Druckkesseln oder Explosionen in chemischen Anlagen nach einer Fehlsteuerung der Produktion, auch Menschenleben gefährdet werden können, verleiht OT-Attacken eine ganz neue Qualität: Auf einmal drohen nicht nur finanzielle Verluste, sondern der Tod".[14]

5 Handlungsperspektiven: Cyberattacken abwehren, Risiken in der digitalen Sphäre neutralisieren, wirksame Präventionsmaßnahmen durchsetzen

Die entscheidende Zukunftsfrage lautet: Wie lassen sich die zuvor beschriebenen Cyberangriffe abwehren, wie kann dafür gesorgt werden, dass die aus solchen Angriffen resultierenden Schädigungen – die die Wirtschaft, öffentliche Einrichtungen und

letztlich das gesamte Gemeinwesen betreffen – unterbunden werden? Auf der Ebene öffentlicher Einrichtungen muss zunächst konstatiert werden, dass insbesondere kleinere Kommunen in Deutschland im Hinblick auf Risiken in der digitalen Sphäre oftmals nicht ausreichend geschützt sind. Der Nachholbedarf ist beträchtlich. Nach Expertenhinweisen müssten, um solche Schwachstellen zu beheben, alle staatlichen Stellen – ob es sich nun um eine Landesbehörde, Kreisverwaltung oder Kommune handelt – mehr Investitionen in die IT-Sicherheit und den Datenschutz vornehmen.[15] Die Notwendigkeit dieser Schritte wird heutzutage von den Entscheidungsträgern in Behörden, Verwaltung und Politik nahezu ausnahmslos eingeräumt. Die Entwicklung von passgenauen Sicherheitsmodellen für komplette IT-Lebenszyklen einschließlich Analyse, Planung, Implementierung und Überwachung sowie die Sicherung der KRITIS im Einklang mit den gesetzlichen Vorgaben und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) schreitet folgerichtig voran, um die erheblichen Rückstände früherer Zeiten aufzuholen. Die entsprechenden Maßnahmen umfassen auch spezielle Modellierungen unterschiedlicher Risikoszenarien, sog. Vulnerabilitäts- und Penetrationstests (System- und Anwendungs-Checks auf Schwachstellen und mögliche Einfallstore für Hacker) sowie die Konzeption, Realisierung und Kontrolle der stetig dominanter werdenden Cloud-Verlagerungen.[16] Die im Juli 2022 vom Bundesinnenministerium vorgestellte Cybersicherheitsagenda unterstreicht die grundsätzliche Dringlichkeit derartiger und kontinuierlich auszubauender Maßnahmen. Kernelemente der Cybersicherheitsagenda sind eine neu organisierte Cybersicherheitsarchitektur mit einer führenden Rolle des Bundes, erweiterte Befugnisse für die Sicherheitsbehörden, um Cyberattacken abwehren zu können, die konsequente Bekämpfung und strafrechtliche Ahndung von Cyberkriminalität, aber auch die Stärkung der deutschen Cybersicherheitsforschung zur Erhöhung der sog. Cyber-Resilienz.[17]

Technischer Nachholbedarf in der IT-Sicherheit findet sich mithin auch in zahlreichen privatwirtschaftlichen Unternehmen. Eine besondere Vulnerabilität vieler Produktionsanlagen rührt daher, dass die Technik zum Teil bereits Jahrzehnte alt ist: „Gerade in der Industrie sind Investitionszyklen von 30 bis 40 Jahren keine Seltenheit. Damit stammen Maschinen und Steuertechnik vielfach noch aus Zeiten, in denen die Vernetzung der Anlagen übers Internet oder gar die Auswertung der Betriebszustände mithilfe intelligenter Analysesoftware noch völlig irrelevant waren. Weil die Technik meist allenfalls intern vernetzt und damit gegen externe Zugriffe geschützt war, spielten mögliche Hackerbedrohungen jahrzehntelang keine Rolle. In Zeiten der allumfassenden Digitalisierung der Produktion, einschließlich der angejahrten Altsysteme, rächt sich das jetzt“.[18] Es ist durchaus irritierend, dass Deutschland bei der digitalen Sicherheit internationalen Standards „hinterherhinkt“, obwohl es hinsichtlich der weltweiten Handelsbeziehungen in den zurückliegenden Jahren stets einen der vordersten Ränge einnehmen konnte.[19]

Die aufgeworfene Zukunftsfrage nach der wirksamen Unterbindung von Cyberattacken und deren gesamtwirtschaftlichen und gesellschaftlichen Schäden lässt sich also nicht nur für öffentliche Einrichtungen, sondern ebenso auf Seiten von Unternehmen in Deutschland im Sinne einer durchgreifenden sicherheitstechnischen Optimierung beantworten. Eine entscheidende Rolle kommt dabei den Entscheidungsträgern und Führungskräften sowie der Organisationsentwicklung in den Unternehmen zu. Auf dieser personellen und organisatorischen Ebene „hapert“ es allerdings nach wie vor. Das notwendige Gefahrenbewusstsein scheint oftmals nur rudimentär ausgeprägt zu sein. Nach aktuellen empirischen Erhebungen „fehlt offenbar die nötige Sensibilität für den Schutz der Technik: Nicht einmal jedes fünfte Unternehmen hat [...] bisher ein eigenes Cybersicherheitsbudget für den Schutz der OT-Systeme“[20] – solch ein Erhebungsbefund sollte aufrütteln, da ja namentlich bei Industrieunternehmen die Zuverlässigkeit von digital eingebundenen Steuerungssystemen für die Betriebssicherheit und damit auch für den wirtschaftlichen Erfolg von essenzieller Bedeutung sind. Hinweise zum Gefahrenbewusstsein und zur Risikosensibilität machen deutlich, wie wichtig der Faktor Mensch bei dem Ringen um Cybersicherheit bzw. bei der wirksamen Abwehr derartiger, in Unternehmen und anderen Organisationen unentwegt erfolgenden Angriffe ist. Menschliches Fehlverhalten kann die technischen Potenziale einer noch so guten Cyberabwehr unterminieren und leider geschieht dies tatsächlich immer wieder. So weisen Studiendaten darauf hin, dass annähernd jeder zweite kritische Cybersicherheits-Vorfall oder -Hack das Resultat von Unaufmerksamkeit oder nicht ausreichender Schulung von Mitarbeitern war.[21] Es ist davon auszugehen, dass Mitarbeiter in Unternehmen und Organisationen oftmals nicht wirklich realisieren, dass Cyberbedrohungen sehr ernst zu nehmen sind, dass derartige Attacken gravierende Konsequenzen auf innerbetriebliche/-organisatorische Abläufe haben und letztlich den eigenen Arbeitsplatz gefährden können.

Mithin ist es nicht sinnvoll, primär eine Defizitperspektive einzunehmen, Menschen also vorrangig als „Sicherheitslücke“ zu betrachten. Vielmehr sollte der Mensch als aktiver „Abwehrschirm“ und „Sicherheitsfaktor“ gegen Cyberattacken erkannt werden. Damit Menschen diese Rolle einnehmen können, bedarf es in Unternehmen, Organisationen und Institutionen gezielter Aus- und Weiterbildung sowie einer geeigneten Aktivierung der Risikoerkenntnisfähigkeit von Mitarbeitern. Der Auf- und Ausbau eines entsprechenden Problem- und Sicherheitsbewusstseins im Verbund mit regelmäßigen Schulungen sind „wichtige präventive Maßnahmen um den ‚Sicherheits-Faktor Mensch‘ zu stärken. Relevante Gefährdungen müssen bekannt sein und die Erwartungshaltung hinsichtlich der Informationssicherheit in dem Unternehmen oder der Institution sollte klar kommuniziert werden. So wird die Grundlage für einen sensiblen Umgang mit Daten und IT-Informationssicherheit gelegt“.[22] Man spricht in diesem Zusammenhang auch von „Awareness“ als elementarer Sicherheitsmaßnahme. Awareness beinhaltet, dass zunächst das Problembewusstsein für Cybersicherheit erlangt werden muss, um darauf aufbauend die erforderlichen Verhaltensänderungen für die digitale Ebene umsetzen zu können.[23]

Sowohl Einzelfirmen und -organisationen als auch übergeordnete Institutionen und Verbände sind gefordert, ihre Mitarbeiter im Hinblick auf diese Awareness und konkrete Handlungskompetenzen zu schulen und kontinuierlich weiter zu qualifizieren. Im Bereich der Finanzwirtschaft, namentlich bei Banken, die für die Aktivitäten von Cyberkriminellen ein häufiger gewähltes Ziel

darstellen, werden entsprechende Maßgaben umgesetzt. Die sich immer wieder ändernden Bedrohungslagen und Begehungsformen der Cyberkriminalität machen eine entsprechend flexible Anpassung bzw. Neuentwicklung von Schulungs- und Weiterbildungsprogrammen erforderlich. In der genossenschaftlichen Qualifizierung und Weiterbildung werden diese Herausforderungen aktiv angegangen, um hinsichtlich IT/Digitalisierung eine stetig aktualisierte und damit belastbare Wissensbasis sowie die notwendigen Handlungskompetenzen auf der Entscheiderebene, bei Fachkräften und anderen Mitarbeitern zu gewährleisten. Qualifizierungsmaßnahmen richten sich hier sowohl an die Mitarbeiter von Genossenschaftsbanken als auch genossenschaftlich verankerten Organisationen weiterer Branchen und zielen insbesondere auf ein tragfähiges Informationssicherheits- und Risikomanagement ab, das im Regelbetrieb Cybergefahren identifizieren und wirksam neutralisieren kann. Dabei wird auch die Vermittlung von strukturellen Grundlagenkenntnissen zur digitalen Transformation sowie von entsprechenden Handlungskompetenzen (Digital Leadership, Personal- und Organisationsentwicklung) angestrebt.

Bildrechte: Davide Oliveira.

Anmerkungen

1. Viktoria Schäfer ist Master of Science und wurde an der Steinbeis-Hochschule Berlin promoviert. Sie ist als Vorstandsvorsitzende und wissenschaftliche Leiterin des genossenschaftlichen Forschungsinstituts ADG Scientific-Center für Research and Cooperation mit Sitz in Montabaur tätig. Yvonne Zimmermann ist Dipl.-Bankbetriebswirtin (ADG), Master of Leadership and Organisational Development und wurde an der Universität Hohenheim promoviert. Sie übernahm 2016 den Vorstandsvorsitz der Akademie Deutscher Genossenschaften (ADG) in Montabaur.
2. Rüdiger, Thomas-Gabriel (2022): Herausforderungen der Cyberkriminologie. Die Kriminalpolizei, Ausgabe 2/2022, S. 13-18.
3. Kemper, Klaus (2022): Computerprävention. Sensibilisierung für Gefahren im Netz. Die Kriminalpolizei, Ausgabe 2/2022, S. 11-13.
4. Berthel, Ralph (2022): Identitätsdiebstahl und -missbrauch im Internet. Aktuelle Entwicklungen und Herausforderungen. Die Kriminalpolizei, Ausgabe 2/2022, S. 4-7 sowie Schiemann, Anja (2022): Strafbarkeit des Identitätsdiebstahls durch Phishing, Pharming und Spoofing. Die Kriminalpolizei, Ausgabe 2/2022, S. 7-10.
5. Landeskriminalamt Niedersachsen (2022): ChatScouts – Gemeinsam gegen Cybermobbing. Presseinformation vom 29.6.2022, www.lka.polizei-nds.de/a/presse/pressemeldungen/chatscouts-gemeinsam-gegen-cybermobbing-116254.html.
6. Siehe zur Ausprägung und zu Folgen entsprechender Delikte Huber, Edith (2015): Cybercrime gegen Privatpersonen, in: Guzy, Nathalie, Birkel, Christoph & Mischkowitz, Robert (Hrsg.): Ziele, Nutzen und Forschungsstand. Viktimisierungsbefragungen in Deutschland, Bd. 1. Wiesbaden, BKA, S 393-420.
7. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022): Was sind Kritische Infrastrukturen und warum sind sie so wichtig? KRITIS-Definition der Bundesressorts, Stand Juli 2022, www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html.
8. Berghoff, Tim (2022): Wiedergegebene Expertenaussagen von Tim Berghoff (G Data, Security Manager), in: Künstler, Diana: Cyber Security – Kommunen im Visier. funkschau Business Netzwerk ITK, Beitrag vom 30.6.2022, www.funkschau.de/sicherheit-datenschutz/kommunen-im-visier.195608.html (2 Seiten).
9. Krüger, Janine (2022): Die hybride Bedrohung – Cyberkriege und Cybersicherheit. Effecten Spiegel, Ausgabe 11, S. 4.
10. Angriffe auf deutsche Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen mit einem Schaden von umgerechnet mehr als 1 Mio. USD (Stand Februar 2022, Datenquelle gemäß der folgenden Anmerkung).
11. IW-Daten und Statista-Grafik (2022): Im Visier russischer Hacker – Anteil der bedeutenden Cyberangriffe auf Deutschland und die Ukraine nach Herkunft seit 2011 (in %). Effecten Spiegel, Ausgabe 11, S. 13.
12. Daten gemäß vorgenannter Anmerkung.
13. Kuhn, Thomas (2022): Cyberangriffe gegen Maschinen – Wenn die Smart Factory zur tödlichen Gefahr wird. Wirtschaftswoche, 31.5.2022, www.wiwo.de/technologie/digitale-welt/cyberangriffe-gegen-maschinen-wenn-die-smart-factory-zur-toedlichen-gefahr-wird/28380028.html (2 Seiten).
14. Wiedergegeben bei Kuhn (2022), siehe Anmerkung zuvor.
15. Wiedergegebene Fachmeinungen im Beitrag von Künstler (siehe Anm. weiter oben).

16. Ein kompakter Praxis-Leitfaden für Vulnerabilitäts-/Penetrationstest (IT-Sicherheit) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist abrufbar unter
17. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html.
18. Bundesministerium des Innern und für Heimat (2022): Bundesinnenministerin stellt ihre Cybersicherheitsagenda vor. Nancy Faeser: „Bedrohungslage im Cyberraum wächst jeden Tag“. Pressemitteilung vom 12.7.2022, www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html.
19. Kuhn (2022), siehe Anmerkung weiter vorn.
20. Hinter den USA und Singapur fand sich Deutschland nach jüngeren Daten bereits auf Platz 3 der weltweit registrierten Cyberangriffe auf Unternehmen und Institutionen. Im Jahre 2021 war schon jedes fünfte Unternehmen in Deutschland von mindestens einem Ransomware-Angriff (Schadprogramme insbesondere in Form von Erpressungs- bzw. Verschlüsselungstrojanern) betroffen, wobei 43% dieser Angriffe beträchtliche Auswirkungen auf den Betrieb hatten. Datenquelle: US-Analysehaus 451 Research, redakt. Wiedergabe in ‚boerse online‘, Ausgabe 21/2022, S. 34 („Unternehmen werden zunehmend Opfer von Hackern“).
21. Kuhn (2022), siehe Anmerkung weiter vorn (unter Bezugnahme auf Erhebungsdaten des Beratungsunternehmens Lünendonk & Hossenfelder sowie der Wirtschaftsprüfungsgesellschaft KPMG u.a. aus dem produzierenden Sektor).
22. Gemäß Kaspersky-Daten von 5.000 Unternehmen weltweit („in 46% of cybersecurity incidents in the last year, careless/ uniformed staff have contributed to the attack”). Quelle: The Human factor in IT security: How employees are making businesses vulnerable from within, www.kaspersky.com/blog/the-human-factor-in-it-security/.
23. Cyber-Sicherheitsempfehlungen gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI): „Faktor Mensch“, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/faktor-mensch_node.html.
24. Cyber-Sicherheitsempfehlungen gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI): „Faktor Mensch – Awareness“, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html.