m retail

Sicherheit im Handel

Dossier

unter Mitwirkung von Handelsverband, Innenministerium und Bundeskriminalamt sowie führender Experten von Taylor Wessing, Deloitte, LexisNexis, Risk.Ident, Glory Global Solutions und CRIF

Herausgeber
Oliver Jonke
[o.jonke@medianet.at]

Editorial

Mit Sicherheit handeln

Liebe Leserinnen und Leser!
Das Thema Sicherheit muss nicht unbedingt trocken sein. Es kann sogar sehr spannend aufbereitet werden. Das wissen nicht nur zahlreiche Anbieter von Dienstleistungen in diesem Sektor, sondern auch Autoren. Einer von ihnen ist Marc Elsberg. In seinem 2012 entstandenen Roman „ Blackout – morgen ist es zu spät" erzählt er von den katastrophalen Auswirkungen, die ein breitflächiger Stromausfall in ganz Europa auslöst. Inzwischen wurde es millionenfach verkauft und in 15 Sprachen übersetzt. Wie kommt einem Autor so eine Idee? Zum Beispiel beim Zähneputzen – bei näherer Betrachtung von elektronischen Zahnbürsten, deren Einzelteile aus unterschiedlichen Erdteilen just in time geliefert und assembled werden.

Sicherheit beginnt im Kleinen
Inzwischen haben wir zahlreiche schmerzliche Erfahrungen rund um unterbrochene Lieferketten gemacht – nicht nur durch Cybercrime. Das deutsche Büro für Technikfolgen-Abschätzung hat vor über zehn Jahren ebenfalls bereits die Vulnerabilität unserer Infrastrukturen analysiert. Seitdem wird intensiv an entsprechenden Notfallplänen gearbeitet.

Seit immer schon lebt der Handel davon, dass man sich auf das Vereinbarte verlassen kann, dass die Regeln eingehalten werden. Das bedeutet, dass die Nichteinhaltung von Regeln auch nicht akzeptiert werden muss. Nulltoleranz zahlt sich aus, auch um Auswüchse im Keim zu ersticken. An dieser Stelle ist das sehr aktive Eintreten des Handelsverbandes für Fairness hervorzuheben. So konnte erfolgreich z.B. das Aus für die sog. „22-Euro-Grenze" erstritten werden; zahlreiche Händler aus China hatten davor ihre Waren absichtlich mit zu niedrigen Werten gekennzeichnet und damit illegale Wettbewerbsvorteile ausgenutzt. Europaweit entstanden dadurch Milliardenschäden.

Die aktuelle Sicherheitsstudie auf den folgenden Seiten gibt einen guten Einblick, wie sich die Sicherheit bei uns entwickelt. Dieses Dossier entstand unter Mitwirkung und im Auftrag vom Handelsverband, vom Bundesministerium für Inneres, dem Bundeskriminalamt sowie führender Experten von CRIF, Deloitte, Glory Global Solutions, LexisNexis, Risk.Ident und Taylor Wessing.

Eine spannende Lektüre wünscht Ihnen
Oliver Jonke

Dossier: Sicherheit im Handel

Coverfoto: © Panthermedia.net/jes2uphoto

Inhalt

Impressum

Medieninhaber:
medianet Verlag GmbH
1110 Wien, Brehmstraße 10/4. OG
http://www.medianet.at

Diese Sonderausgabe wurde von **media**net unter Mitwirkung des Handelsverbandes erstellt.

Konzept: Oliver Jonke (Herausgeber)
Kontakt: o.jonke@medianet.at

Leitender Redakteur dieser Ausgabe:
Georg Sander (gs)

Lektorat: Christoph Strolz ***Grafik/Produktion:*** Raimund Appl, Peter Farkas ***Fotoredaktion/Lithografie:*** Beate Schmid ***Druck:*** Bauer Medien Produktions- und Handels-GmbH, 1030 Wien
Erscheinungsort: Wien ***Stand:*** Mai 2023

Für den Inhalt verantwortlich:
Gerald Kühberger, Handelsverband
1080 Wien, Alser Straße 45
Kontakt: office@handelsverband.at

Abo, Zustellungs- und Adressänderungswünsche:

abo@medianet.at
oder Tel. 01/919 20-2100

Vertrauen ist gut, Kontrolle noch besser

Die Behörden arbeiten in Sachen Cybercrime vorbildlich. Allerdings müssen auch Händler ihren Teil dazu beitragen.

WIEN. Die Möglichkeiten, wie Kriminelle Handelsunternehmen um ihr Geld bringen können, nehmen zu. Das zeigt die Sicherheitsstudie 2023, und das weiß Robert Spevak, beim Handelsverband Leiter des Ressorts „Sicherheit im Handel" und Abteilungsleiter Revision, Sicherheit bei Metro, ganz genau: „Wir werden immer digitaler, so auch der Handel. Die Kriminellen lassen sich ständig Neues einfallen."

Schnell passiert

„Wenn sich unser Konsumverhalten insgesamt immer mehr in die Online-Welt verlegt, dann bedeutet das auch, dass die Möglichkeiten für Kriminalität vielfältiger werden", erklärt er.

Was heißt das also für Betreiber eines Webshops? Dass Vorsicht geboten ist. Im Rahmen der Sicherheitsstudie gab ein Drittel der Handelsunternehmen an, dass sie schon mehrfach von Cybercrime betroffen gewesen sind. „Viele kleine Betriebe haben ein Bewusstsein für das Thema, allerdings hat ein knappes Drittel angegeben, dass es (noch) keine Präventionsmaßnahmen gibt", stellt er fest.

Anscheinend vertraut der eine oder andere noch zu viel auf sein eigenes Gespür, vielleicht denkt man sich etwas naiv: Mir kann das nicht passieren. „Allerdings geht es sehr schnell", erklärt Spevak aus eigener Erfahrung, „im Arbeitsstrudel klickt man schon einmal ein Phishing-Mail an und wird dann Opfer von Online-Betrug. Den monetären Schaden hat der Händler, den Zeitaufwand der vermeintliche Konsument. Der Imageschaden liegt auch beim Unternehmen, obwohl man nichts dafür kann."

© Katharina Schiffl

Erfahrung Robert Spevak weiß sehr gut, worauf es im Handel in Sachen Sicherheit ankommt.

Wovon sind Händler also betroffen? Beispielsweise von Identitätsdiebstahl. So wird bestellt und abgestritten, die Ware jemals erhalten zu haben; es sei eben die falsche Adresse: „Diese Art von Betrug hat enorm zugenommen. Es ist für den Händler schlecht, weil die Ware weg ist, und der, dessen Identität geklaut wurde, muss sich um Aufklärung bemühen."

Prävention entscheidend

Spevak verweist auf die Wichtigkeit der Prävention, etwa durch Mehrwegauthentifizierung, verifizierte Zahlungsdienstleister oder die Verweigerung, Kauf auf Rechnung zu akzeptieren. Vertrauen sei hierbei gut, Kontrolle noch besser, aber „klar muss sein, dass Sicherheit auch Geld kostet".

Anzeigen, anzeigen, anzeigen

Auch der Diebstahl im stationären Handel sei weiterhin ein Thema. Manche versuchen, zwei gleichgefüllte Wagerl an der Kassa vorbeizubekommen und einen nicht zu zahlen, andere manipulieren Verpackungen. Solche Handlungen sollten immer zur Anzeige gebracht werden. Auch die Zusammenarbeit mit dem BMI namens „Gemeinsam.Sicher" kann eine gute Prävention für den Handelsbetrieb darstellen: „Nur wenn ein Diebstahl angezeigt wird, können die Behörden tätig werden und die Muster der Tätergruppen analysieren. Unsere Sicherheitsbehörden funktionieren gut und sind up-to-date, was die Kriminalitätsmaschen betrifft. Anzeigen sind entscheidend, um die Täter fassen zu können, die Methoden besser zu verstehen und Kriminalität im stationären wie im Onlinehandel effektiv zu verhindern."

> *„Jede einzelne Anzeige hilft, um die Täter zu fassen, die Methoden besser kennenzulernen und somit zu verhinden."*
>
> **Robert Spevak**
> *Leiter Ressort „Sicherheit im Handel", Handelsverband*

© Katharina Schiffl

Handel: „Krisenresilienter Versorger und Jobmotor“

Rainer Will findet als Geschäftsführer des Handelsverbandes lobende Worte für die Branche und mahnende wegen Cybercrime und Richtung Politik.

Die letzten Jahre waren für den Handel alles andere als einfach und trotzdem konnte die Handelsbranche die Menschen mit dem Notwendigsten und noch mehr versorgen. Nach den Monaten mit starker Inflation scheint diese sich einzubremsen – somit ist Handelsverband-Geschäftsführer Rainer Will „vorsichtig optimistisch“. Es gibt Lob, aber auch mahnende Worte in mehrere Richtungen.

medianet: *Während der Pandemie hat sich der Handel als Teil der kritischen Infrastruktur als verlässlicher Partner präsentiert. Die Herausforderungen – Stichwort Teuerung – reißen nicht ab. Wenn der Euro öfters umgedreht werden muss, welchen Faktor spielt die Verlässlichkeit des heimischen Handels für die Menschen punkto Sicherheit?*
Rainer Will: Wir hatten in den letzten drei Jahren mit multiplen Krisen zu kämpfen, haben eine Pandemie mit fünf Lockdowns überstanden, in der sich der heimische Handel als krisenresilienter Nahversorger und Jobmotor bewährt hat. Unsere Branche hat die Erstausstattung der gesamten Bevölkerung mit Schutzmasken gestemmt und eine heraus-

© Katharina Schiffl

ragende Rolle beim Aufbau des Corona-Testsystems gespielt. Auch nach der Pandemie werden die Herausforderungen nicht weniger. Aktuell beschäftigt uns die Teuerung sowie der flächendeckende Personalmangel, und die globale Klimakrise wirft ebenfalls ihre Schatten. Dennoch hat sich die Stimmung der Händler ebenso wie das Konsumentenvertrauen seit Oktober 2022 kontinuierlich verbessert. Die Inflation hat sich zuletzt im März auf 9,2 Prozent etwas eingebremst. Die Konsumstimmung hellt sich auf, und unser wirtschaftlicher Ausblick für das zweite Quartal ist vorsichtig optimistisch. Sicherheit im Handel wird in Österreich großgeschrieben, das zeigt etwa der gemeinsame Blackout-Vorsorge-Plan des heimischen Lebensmittelhandels.

> *Sicherheit im Handel wird in Österreich großgeschrieben; das zeigt etwa der gemeinsame Blackout-Vorsorge-Plan des heimischen Lebensmittelhandels.*
>
> **Rainer Will**
> *Geschäftsführer Handelsverband*

medianet: *Gerade in unsicheren Zeiten sind on- und offline verlockende Angebote zu finden. Welchen Vorteil bietet der heimische Handel aus Ihrer Sicht gegenüber (internationalen) Glücksrittern?*
Will: Wer in österreichischen Geschäften einkauft, kann sich darauf verlassen, dass unsere hohen Standards insbesondere beim Umwelt- und Klimaschutz, der Gentechnikfreiheit sowie beim Einsatz von Pflanzenschutzmitteln eingehalten werden. Heimische Händler zahlen gute Löhne, vielfach mit Überzahlung und auch Zuschläge, für die hierzulande Steuern entrichtet werden, und damit tragen wir entscheidend zum Gemeinwohl bei – Stichwort Fairer Handel. In Österreich gekauft, ist also richtig gut gekauft, sichert 625.000 Arbeitsplätze, stärkt unsere Wirtschaft, schützt die Umwelt und sorgt für ein gutes Gewissen.

64%

Online
Fast zwei Drittel der Händler (64%) waren bereits von Cybercrime und Betrug im Netz betroffen, mit 34% die Hälfte mehrfach – so entstehen jährlich 16 Mio. Euro Schaden.

medianet: *Die Kontrolle im Web gestaltet sich schwierig, von 2020 auf 2021 sind Cybercrime-Delikte stark angestiegen. Nun sind die Covid-Einschränkungen vorbei, beobachten Sie hierbei einen Rückgang?*
Will: Im Gegenteil, Cybercrime und Bestellbetrug verzeichnen weiterhin enorme Zuwachsraten. Laut unserer aktuellen Sicherheitsstudie wurden bereits 64 Prozent aller heimischen Onlinehändler Opfer von Betrug, ein Drittel sogar mehrmals.

medianet: *Vor welchen Sicherheitsherausforderungen steht die Handelsbranche aktuell?*
Will: Im stationären Handel zählen der klassische Ladendiebstahl, die Bezahlung mit Falschgeld sowie Vandalismus im Shop zu den größten Sicherheitsherausforderungen. Im Digitalbereich treten vor allem Phishing, Malware-Angriffe, Ransomware sowie Cyber-Erpressung immer häufiger auf. Beunruhigend ist auch, dass bereits ein Viertel aller Konsumenten Opfer von Fake-Webshops geworden sind.

Relevanz
Handelsverband-Geschäftsführer Rainer Will trifft Bundeskanzler Karl Nehammer.

medianet: *Aus Brüssel kommen immer wieder Vorgaben, welche die Kundenbeziehung verändern, mit der Intention, rechtliche Sicherheit zu geben. Wie beurteilt der Handel diese Entwicklung?*
Will: Solange die Vorgaben praxistauglich und unbürokratisch umsetzbar sind, begrüßen wir das. Beispielsweise hat die EU auf die Gefahr von Online-Betrug reagiert und in ihrer Zahlungsdienste-Richtlinie (PSD2) die 2-Faktor-Authentifizierung (2FA) vorgeschrieben. Diese besagt, dass sich Kunden bei Bezahlung über das Internet zumindest doppelt identifizieren müssen – etwa mittels Passwort und SMS TAN. Seit März 2021 können Online-Zahlungen nur noch mit Starker Kundenauthentifizierung durchgeführt werden. Das sorgt für mehr Sicherheit im europäischen Zahlungsverkehr. Der Handelsverband unterstützt Webshops mit dem eCommerce Gütesiegel Trustmark Austria sowie im Rahmen der Initiative ‚Gemeinsam sicher einkaufen' mit kompetenten Partnern dabei, sich stationär wie digital optimal aufzustellen.

82%

Stationär
Eine große Mehrheit der Händler (82%) gibt an, bereits Opfer von Kriminalität im stationären Handel geworden zu sein, 40% sogar mehrfach. Die Schadenssumme: 500 Mio. Euro jährlich.

Top 5-Delikte im Netz

Händlersicht
1. Datendiebstahl/Phishing
2. Malware-Angriffe
3. Cyber-Erpressung
4. Ransomware
5. Botnetze & DDoS-Angriffe

Konsumenten
1. Schadsoftware (Viren)
2. Datendiebstahl/Phishing
3. Betrug bei Online-Transaktionen
4. Digitale Erpressung
5. Identitätsdiebstahl

Sicher im (Web-)Shop

Nach dem Corona-Boom pendelt sich der Absatz im Onlinehandel ein. Auch der stationäre Handel hat sich stabilisiert – Risiken gibt es da und dort.

Wer heutzutage nah an der Kundschaft sein will, kommt um einen Online-Shop kaum umhin. Damit steigen aber auch die möglichen Gefahren. Zwei Drittel der heimischen Handelsbetriebe waren bereits Opfer von Kriminalität im Netz, ein Drittel sogar mehrfach, so ein Kernergebnis der Sicherheitsstudie 2023. Die Verluste aufgrund von Cybercrime belaufen sich hierzulande mittlerweile auf mehr als 16 Mio. Euro jährlich.

„Nach dem Pandemie-bedingten Höhenflug im Bereich eCommerce sehen wir jetzt eine Konsolidierung der Umsätze. Die kriminellen Handlungen im Netz nehmen hingegen fast ungebremst zu“, sagt Stephan Mayer-Heinisch, Präsident des Österreichischen Handelsverbandes.

Sichtweise
Wir wollen einkaufen, wann, wo und wie es uns gerade passt. Ehrlichkeit und Transparenz sollten dabei ein ständiger Begleiter sein. Dem ist aber (oft) nicht so.

Im ersten Pandemiejahr 2020 sind die Online-Umsätze noch um stolze 17,1% nach oben geklettert. 2022 musste der heimische eCommerce im Zuge der Teuerungskrise erstmals in seiner Geschichte ein reales Minus von fast 8% verkraften. Heuer gehen die Experten wieder von einem moderaten Wachstum aus.

Mehr Schaden

Aus der vom Handelsverband in Kooperation mit dem Innenministerium durchgeführten Sicherheitsstudie 2023 geht hervor, dass 64% der österreichischen Online-Händler im vergangenen Jahr Opfer von Online-Betrug wurden; bei größeren Unternehmen waren es sogar drei von vier. Zu den gängigsten Formen von Cybercrime im Handel zählen aktuell Phishing (61%), Malware-Angriffe (52%), Cyber-Erpressung durch Hacker (32%), Ransomware (28%) und Botnetze bzw. DDoS Angriffe (16%).

Im eCommerce werden häufig Waren bestellt, obwohl den Kunden bewusst ist, dass die Rechnung später nicht beglichen werden kann (57%). Weit verbreitet ist auch die Angabe der Identität einer anderen Person (51%) bzw. die Angabe verfälschter Namens- oder Adressdaten (50%). Oftmals streiten Kunden auch ab, die Ware bestellt zu haben (47%), oder es

500

Millionen
Alleine im stationären Handel verursachen Ladendiebstähle einen jährlichen Schaden von einer halben Milliarde Euro.

© Stephan Doleschal

Über die Sicherheitsstudie

Analysten
Die Sicherheitsstudie 2023 wurde vom Österreichischen Handelsverband in Kooperation mit dem Bundesministerium für Inneres (BMI) durchgeführt.

Teilnehmer
150 Unternehmen aller Handelsbranchen und Größenordnungen (vom Ein-Personen-Unternehmen bis zum Konzern) haben teilgenommen und den Fragebogen vollständig ausgefüllt. Zusätzlich wurden 1.026 Konsumenten befragt. Der Erhebungszeitraum betrug acht Wochen, Studienende war der 31. März 2023.

Weitere Infos auf: *www.sicherheitsgipfel.at*

© Handelsverband

handelt sich um einen Betrug bei der Warenauslieferung/-übergabe (46%). Öfters genannt werden noch Betrügereien im Zusammenhang mit Retouren (40%), Angabe gestohlener Zahlungsdaten (38%) oder Kunden streiten ab, Ware bestellt zu haben, obwohl sie dies getan haben (35%).

Pikantes Detail der Sicherheitsstudie: Im Vorjahr lag nur noch ein Fünftel (18%) der Schadenssummen unter 500 Euro, in 22% der Fälle verloren die Händler hingegen zwischen 5.000 und 10.000 Euro. Auch der Anteil der Fälle mit einem Schaden zwischen 100.000 und einer Million Euro ist von 2% auf 3% angewachsen. Erstmals wurde 2022 die Millionenmarke geknackt – in 3% der Betrugsfälle lag die Schadenssumme über diesem Wert.

Konsumentenperspektive
Darüber hinaus wurde im Rahmen der Sicherheitsstudie auch die Perspektive der Konsumenten betrachtet: Ein Drittel der heimischen Verbrauchern hat bereits negative Erfahrungen mit Schadsoftware wie Viren oder Trojanern gemacht. 20% waren schon von Datendiebstahl durch Phishing-Angriffe betroffen, weitere 14% waren Opfer von Betrug bei Online-Transaktionen. 78% der Österreicher versuchen, sich mit Virenschutz-Programmen vor Cyberangriffen zu schützen. 58% setzen auf regelmäßige Software-Updates, und immerhin 63% haben eine Firewall implementiert. Beunruhigend ist, dass bereits fast ein Viertel aller Konsumenten (26%) Opfer von Fake-Webshops geworden sind. „Die Betrüger sind leider sehr raffiniert, und kriminelle Handlungen betreffen nicht nur die Händler, sondern auch deren Kunden", so Stephan Mayer-Heinisch (Bild).

Online-Schutz wichtig
Im stationären Handel gibt es oftmals Präventionsmaßnahmen, das ist auch online entscheidend. Welche Maßnahmen gibt es? 61% setzen auf sichere Zahlungsoptionen. Auf Platz zwei rangiert mit 42% die Einschränkung von Lieferoptionen – die Handelsbetriebe liefern zum Beispiel nur innerhalb des eigenen Landes. Rang drei geht an die Identitätsprüfung (36%), gefolgt vom Bonitätscheck (33%) und Hotlists, also eigenen Datenbanken mit kritischen Adressen (30%).

Allerdings gibt es hierbei auch markante Unterschiede. Während etwa bei den größeren Betrieben 58% auf eine Identitäts- und 55% auf eine Bonitätsprüfung zur Risikominimierung setzen, sind es bei den KMU-Webshops nur 16% respektive 12%. Stolze 42% der größeren Onlinehändler verwenden eine „Hotlist" – auch dieses Schutzinstrument kommt bei kleineren Unternehmen mit 19% weit seltener zum Einsatz.

Stationär geht mehr
Betroffen ist auch der stationäre Handel. Dort verursachen Ladendiebstähle einen jährlichen Schaden von rund 500 Mio. Euro. 82% der für die Sicherheitsstudie 2023 befragten Händler mit physischen Geschäften haben bereits Erfahrung mit Kriminalität im eigenen Shop gemacht, 40% sogar mehrfach.

Die Liste der häufigsten Vergehen wird angeführt vom klassischen Ladendiebstahl (89%), gefolgt von der Bezahlung mit Falschgeld (43%), organisierter Bettelei und Vandalismus im Shop (je 22%) sowie Bandenkriminalität (18%).

Acht von zehn Händlern haben konkrete Maßnahmen zum Schutz vor Kriminalität im eigenen Geschäft in Verwendung. Am häufigsten setzen die Betriebe auf Mitarbeiterschulungen (63%), Videoüberwachung (59%), das Verschließen aller Betriebsräume (52%), die Nutzung von Warensicherungsanlagen und Einbruchmeldeanlagen (44%) sowie besondere Maßnahmen für „Hot Products" (40%).

Betrug vermeiden
Wer (off- und) online mehr Sicherheit will, bietet beispielsweise Kartenzahlung an. In Webshops ist die Kreditkarte mit vier Fünftel die gängigste Zahlungsmethode. Wenn es dann doch zu einem Betrug kommt, hilft die Polizei.

„Für uns als Handelsverband ist es entscheidend, das Bewusstsein für die verschiedenen Kriminalitätsformen zu schärfen", meint Präsident Mayer-Heinisch abschließend. „Alle Seiten wollen Sicherheit und es gibt verschiedene Wege, sie zu erreichen: Durch Präventionsmaßnahmen vor Ort oder etwa durch das Webshop-Gütesiegel des Handelsverbandes."

Schadenssummen

Schaden durch Onlinebetrug	
unter 500 €	18%
unter 1.000 €	18%
unter 5.000 €	9%
unter 10.000 €	22%
unter 100.000 €	15%
unter 1 Mio. €	3%
über 1 Mio. €	3%

Quelle: Handelsverband

© Panthermedia.net/sdecoret

Cybercrime: Laufend neue Vorgehensweisen

Die Kriminalität im Internet steigt weiter an, die Polizei mahnt den Faktor Sicherheit im Onlinehandel ein. Die Initiative „Gemeinsam.Sicher“ unterstützt Händler.

WIEN. Die Digitalisierung öffnet uns weltweit viele Türen, zuweilen leider mit einem bitteren Beigeschmack. Denn egal ob es sich um Schadsoftware, Datendiebstahl oder digitale Erpressung handelt, die Möglichkeiten von Cyberkriminellen nehmen rasant zu – auch im Onlinehandel. Wenngleich die eCommerce-Umsätze im Vorjahr erstmals in den letzten 20 Jahren zurückgegangen sind, wächst das Risiko für Betrug weiter. Das ist auch eine zentrale Erkenntnis der Sicherheitsstudie 2023, die vom Handelsverband in Kooperation mit dem Innenministerium und dem Bundeskriminalamt durchgeführt wurde.

Die Digitalisierung ist aus dem privaten und geschäftlichen Alltag nicht mehr wegzudenken. Darauf haben sich auch Kriminelle eingestellt und ihr Treiben großteils in das Internet verlagert. Auch im digitalen Raum kommt es zu den verschiedensten Formen von Kriminalität. Die Beschränkungen rund um die Covid-19-Pandemie haben, im Gegensatz zu den herkömmlichen Eigentumsdelikten, die Entwicklungen im Cyberbereich noch weiter beschleunigt.

© Panthermedia.net/gualtiero boffi

Beachten
Auch die Kriminalität im stationären Handel ist im Auge zu behalten, meint General Andreas Holzer, Direktor des Bundeskriminalamts.

© Fotostudio Semrad/Andreas Semrad

2022 wurde in der Kriminalstatistik im Bereich der Cybercrime ein Höchstwert von 60.195 Anzeigen verzeichnet. Besonders der Online-Handel ist von Betrugsdelikten betroffen. Die Aufklärungsquote bleibt – gerade im Hinblick auf die gestiegenen Zahlen – konstant hoch. Das besagt der Lagebericht des Bundeskriminalamts (BK).

Starker Anstieg

Betrug im Netz ist keine Einbahnstraße: Mehr als ein Fünftel der Konsumentinnen und Konsumenten haben laut Sicherheitsstudie schon Erfahrungen mit Fake-Webshops gemacht.

„Im Kampf gegen die Internetkriminalität setzen wir als Sicherheitsbehörde sowohl in der Strafverfolgung als auch der Prävention auf stete Fortbildung, Modernisierung und eine möglichst umfassende Vernetzung mit den diversesten Stakeholdern“, erklärt Innenminister Gerhard Karner. „Ganz nach der Prämisse: Das beste Delikt ist jenes, das schon vorab verhindert werden konnte.“

Sicherheit
Die Gefahr von Cyber-Attacken bleibt leider hoch.

Aber was fällt eigentlich alles unter Cybercrime? Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie zum Beispiel bei der Datenbeschädigung, dem Hacking oder Angriffen auf Dienste (DDoS-Attacken). Betrügerischer Datenverarbeitungsmissbrauch gehört auch dazu – hier verzeichnete das BK 2022

© BMI/Karl Schober

massive Anstiege. Hauptgrund hierfür sind die zunehmende Verlagerung des täglichen Lebens in das Internet sowie die Schaffung neuer internetbasierter Zahlungsmöglichkeiten. Die betrügerische Verwendung von Near Field Communication (NFC) bei Bankomat- und Kreditkarten mache hierbei den größten Anteil der Anzeigen aus. Auch die Fälle von Phishing seien stark angestiegen, heißt es aus dem BK. Unter Cybercrime im weiteren Sinne werden Straftaten verstanden, bei denen die Informations- und Kommunikationstechnik als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, wie zum Beispiel Betrugsdelikte, Drogenhandel im Darknet, Online-Kindesmissbrauch, Cybergrooming oder Cybermobbing. „Jene Bereiche der traditionellen Kriminalität, in denen Digitalisierung und IT keine Rolle mehr spielen, werden somit immer kleiner", so Karner.

Konstante Aufklärung

Cybercrime in all seinen vielfältigen Erscheinungsformen stieg von 46.179 angezeigten Delikten im Jahr 2021 auf 60.195 im Jahr 2022 – dies bedeutet ein Plus von 30,4 Prozent. Trotz des beachtlichen Zuwachses konnte die prozentuelle Aufklärungsquote mit 33,9 Prozent sehr hochgehalten werden. Den größten Posten nimmt der Internetbetrug ein, er hat mit 27.629 Anzeigen einen neuen Höchststand erreicht. „Auch wenn wir die Beobachtung machen, dass sich die Kriminalität in vielen Bereichen in das Internet verlagert, so dürfen wir den stationären Handel, als essenziellen Teil der Wirtschaft in Österreich, keinesfalls außer Acht lassen", betont General Andreas Holzer, Direktor des Bundeskriminalamts.

Mahner

Manuel Scherscher, stellvertretender Direktor des Bundeskriminalamts und Leiter der Initiative „Gemeinsam. Sicher", warnt vor Schwachstellen im Bestellprozess von Webshops.

© BK/Fröhlich

Warnende Worte

Rainer Will, Geschäftsführer des Handelsverbands, bringt das pandemiebedingte Wachstum an Webshops und Onlinebestellungen mit den häufigeren Delikten, neuen Betrugsmaschen und deutlich höheren Schäden in Zusammenhang und warnt: „Handlungsbedarf ist gegeben. Im Vorjahr waren bereits zwei Drittel der heimischen Händler Opfer von Betrug im Netz, ein Drittel sogar schon mehrmals. Damit steht Internetbetrug weit oben auf der Liste potenzieller Bedrohungen für den Handel. Die Schäden nehmen zu und gehen teilweise in die Millionen." Ähnlich sei die Situation auf Konsumentenseite: Jeder Zweite schätze die Gefahren im eCommerce als hoch ein. Für Online-Shopper zähle Sicherheit mittlerweile zu den wichtigsten Kaufkriterien.

Der eCommerce-Boom sei auch den Kriminellen nicht entgangen, mahnt Manuel Scherscher, stellvertretender Direktor des BK und Leiter der Initiative Gemeinsam.Sicher: „Sie nutzen die vermeintlichen Schwachstellen im Bestellprozess von Webshops für ihre Machenschaften oder verwenden real existierender Identitäten beim Kauf auf Rechnung missbräuchlich."

Prävention

„Das beste Delikt ist jenes, das schon vorab verhindert werden konnte", weiß Gerhard Karner, Bundesminister für Inneres.

Prävention und Kooperation

Eines zeigt die Kriminalitätsstatistik deutlich: „Es ist aus Sicht der Polizei unumgänglich, ein besonderes Augenmerk auf den Faktor Sicherheit im Onlinehandel zu werfen, wobei auch der stationäre Handel im Fokus vieler Täter steht", betont Scherscher. Die Polizei registriert laufend neue Vorgehensweisen der Kriminellen, weshalb neben der Repression, der Verfolgung der Täter, auch vermehrt auf Präventionsmaßnahmen gesetzt wird. Im Schadensfall kann in jeder Polizeiinspektion eine Anzeige erstattet werden. „Mit der Initiative ‚Gemeinsam.Sicher' im Onlinehandel haben das Bundeskriminalamt und der Handelsverband bereits vor Jahren eine Plattform geschaffen, welche die enge Zusammenarbeit zwischen dem österreichischen Handel und der Polizei intensiviert und fördert. Diese Sicherheitspartnerschaft stellt ein wesentliches Element dar, die Sicherheit im Onlinehandel weiter zu verbessern", erklärt Scherscher das Ziel der Kooperation.

Mehr Details

Nähere Informationen zum Thema Cybercrime sowie den Cybercrime Report des BMI unter: *www.bundeskriminalamt.at/cybercrime*

Das Zauberwort heißt Vertrauen

Um sich von unseriösen Angeboten abzugrenzen, sollten Onlinehändler auf Transparenz, vertrauensbildende Maßnahmen und Gütesiegel setzen.

Österreichische Gütesiegel für Webshops

Ausstellende Institution	Handelsverband	Trusted Shops GmbH	ÖIAT
Zusätzliches EU-Siegel	✓	–	–
Sitz	Wien	Köln	Wien
Gründungsjahr	1995	1999	2000
Basis für Zertifikat	Rechtskonformität	Rechtskonformität	Rechtskonformität
Mindestvertragsdauer	1 Jahr	1 Jahr	1 Jahr
Prüfintervall	jährlich	Ermessen / Stichproben	jährlich
Einmalige Prüf- bzw. Setup-Gebühr	400 Euro	99 Euro	550 - 1.650 Euro**
Nutzungsgebühr jährlich	480 - 1080 Euro* (400 Euro für Mitglieder)	ab 1.428 - +3.348 Euro*	550 - 1.650 Euro**
Bearbeitungsgebühr bei Schadensfällen	0 Euro	25 Euro	0 Euro
Rechtstexte mit Abmahnschutz/ Haftungsübernahme (gegen Aufpreis)	+107 Euro (via Partner)	+ca. 360 Euro (als PRO Paket)	–
Persönlicher Ansprechpartner	inkludiert	+ca. 360 Euro (als PRO Paket)	inkludiert

© Handelsverband

WIEN. Transparenz, Sicherheit, der Einsatz von Kundenbewertungen und Gütesiegeln stellen bei Webshops die wichtigsten Säulen dar, um sich von unseriösen Angeboten abzugrenzen. Befeuert durch die Coronapandemie, setzen mittlerweile auch vermehrt kleine Handelsbetriebe auf einen eigenen digitalen Kanal. Insbesondere jene Webshops, die noch vergleichsweise unbekannt sind, müssen ihre Kunden umso intensiver davon überzeugen, dass sie in einem seriösen Onlineshop gelandet sind. Der erste Eindruck ist hier der wichtigste. Ansprechendes Design, gute Usability, eine übersichtliche Struktur und hochwertige Produktbilder spielen eine entscheidende Rolle.

Kundenempfehlungen

Vertrauen kann am einfachsten mithilfe unabhängiger Dritter aufgebaut werden. Dafür eignen sich vor allem Kundenbewertungen sowie eCommerce-Gütesiegel, wie auch die Sicherheitsstudie 2023 von Handelsverband und Bundeskriminalamt belegt. Kundenbewertungen im Internet sind zu vergleichen mit klassischer Mund-zu-Mund Propaganda im stationären Handel. Wenn bereits viele andere in einem Onlineshop gekauft haben und eine positive Bewertung hinterlassen haben, steigt das Vertrauen. Nichts ist aussagekräftiger als Empfehlungen von anderen Käufern.

Siegel

Welches Gütesiegel bietet welche Leistung? Jenes vom Handesverband überzeugt.

Orientierungshilfe

Gütesiegel, etwa „Trusted Shops" oder das Trustmark Austria des Handelsverbandes, bieten eine wertvolle Orientierungshilfe, um auf einen Blick zu erkennen, ob es sich um einen vertrauenswürdigen Webshop handelt. Die ausstellenden Institutionen prüfen die jeweiligen Shops im Hinblick auf generelle Qualitätsstandards, Sicherheit oder Rechtskonformität. Die Kunden sollten durch einen Klick auf das angezeigte Gütesiegel auf die Webseite des Siegel-Betreibers weitergeleitet werden. Auf dieser sind in der Regel alle zertifizierten Shops aufgelistet. So kann rasch überprüft werden, ob der Onlineshop das Gütesiegel befugterweise auf der Website platziert hat.

Weitere Informationen auf: www.trustmark-austria.at

© Stephan Doleschal

Um sich von unseriösen Angeboten abzugrenzen, sollten Händler auf Transparenz und Gütesiegel setzen.

Patricia Grubmiller
Head of Legal im Handelsverband

Andreas Schütz ist Partner bei Taylor Wessing.

Peter Lohberger ist Associate bei Taylor Wessing.

„Beratungsbedarf steigt massiv an“

Die Rechtsexperten von Taylor Wessing, Andreas Schütz und Peter Lohberger, analysieren die Lage.

WIEN. Wo ein Schaden auftritt, ist die Frage der Haftung nicht weit. Oder, salopper formuliert: Einer muss schuld sein. Doch es gibt natürlich einiges zu beachten.

Wie es sich mit der Haftung bei Cybercrime-Vorfällen verhält, erklären Andreas Schütz, Partner und Datenschutzexperte bei Taylor Wessing, und Peter Lohberger, Associate bei Taylor Wessing, im Gespräch mit **media**net. Beide befassen sich unter anderem intensiv mit den Themen Datenschutz und Cybercrime.

medianet: *Spiegelt sich die Sicherheitsstudie auch in der anwaltlichen Praxis wider?*
Andreas Schütz: Ja, definitiv. Der rechtliche Beratungsbedarf aufgrund von Cybercrime ist in den letzten Jahren massiv gestiegen. Obwohl es schlussendlich jeden treffen kann, ist festzustellen, dass eine technische wie jedenfalls auch rechtliche Vorsorge den Schaden minimieren kann. Es wäre besser, wenn Anwälte nicht erst bei Eintritt des Schadens gerufen würden.

medianet: *Mit welchen Fällen sind Sie in der Praxis konkret konfrontiert?*
Peter Lohberger: Wir merken einen konstanten Anstieg im Bereich Phishing, Malware, Ransomware und Cyber-Erpressung. Dabei ist der sog. Rechnungsbetrug (hier wird die Kontonummer verfälscht), wie auch die Verschlüsselung bzw. das Downloaden von Daten durch Kriminelle weiterhin stark im Trend; die Schadenssummen sind hier enorm.

medianet: *Was sind die rechtlichen Fragestellungen beim angesprochenen Rechnungsbetrug?*
Schütz: Strafrechtlich wird meist der Rechnungsempfänger betrogen, welcher aufgrund des Betrugs auf eine entsprechend falsche Kontoverbindung eingezahlt hat. Schlussendlich geht es darum, ob die Zahlung nochmals, aber an den richtigen Empfänger mit der richtigen Kontonummer, gezahlt werden muss. Die schuldbefreiende Wirkung einer in gutem Glauben an einen Dritten (z.B. Vorlieferant) geleisteten Zahlung hängt davon ab, ob man selbst mit der gebotenen Sorgfaltspflicht gehandelt hat. Beispielsweise sollte bei einer lang bestehenden Geschäftsbeziehung eine plötzliche Kontoänderung auffallen bzw. zumindest eine telefonische Rückfrage erfolgen. Sofern man fragwürdige Umstände ignoriert, spricht dies oft für eine mangelnde Sorgfalt. Entsprechende technisch-organisatorische Maßnahmen bzw. ein wirksames internes Kontrollsystem könnten wesentlich dazu beitragen, Straftaten zu verhindern.

> *Die schuldbefreiende Wirkung einer in gutem Glauben an Dritte geleisteten Zahlung hängt davon ab, ob man mit der gebotenen Sorgfaltspflicht gehandelt hat.*
>
> **Andreas Schütz**
> *Taylor Wessing*

medianet: *Welche Kosten kommen hier auf die Unternehmen üblicherweise zu?*
Lohberger: Das ist stark vom Einzelfall und Sachverhalt abhängig. Wir arbeiten intensiv mit mehreren Cyberversicherungen zusammen. Je nach Versicherungsmodul werden dabei z.B. die anwaltlichen Kosten bei der Abwehr und Minderung des Schadens, aber auch Haftungsansprüche von Dritten (wie z.B. durch Datenschutzverletzungen) abgedeckt. Umfasst ist üblicherweise die Abwehr von Haftungsansprüchen und Versicherungsschutz im (Verwaltungs-)strafverfahren.

Die digitale Identität

Das Leben spielt sich zunehmend online ab, eine digitale Identität macht den Handel und die Wirtschaft sicherer.

© P19/Lieb.Ich Productions

Starkes Team Martin Sprengeis-Kogler von P19, Ruth Moss und Gerald S. Eder von CRIF, Birigt Kraft-Kinz von P19 (v.l.).

WIEN. So wie wir in der realen Wirklichkeit die Person eindeutig identifizieren können – ein Ausweis und der Fotoabgleich mit der Person, die vor mir steht, reichen dazu –, gilt dieser Anspruch auch im Digitalen. Durch die rasche Digitalisierung, die durch die Covid-pandemie eine Beschleunigung erfahren hat, hat die digitale Identifikation auch an Bedeutung gewonnen.

Eindeutige Identitäten

„Aus dem dringenden Bedarf sind viele verschiedene Identifikations-Methoden und -verfahren von verschiedenen Anbietern entstanden. Dadurch ergibt sich ein Vielfalts-Dilemma", sagt Gerald Sebastian Eder, Director Digital Solutions bei CRIF, einem weltweit agierenden Unternehmen, das datenbasierte Lösungen für Risiko-, Fraud- und Identitätsmanagement anbietet. Die Beispiele sind bekannt: Es gibt Tools, die einen physischen Abgleich digital abbilden oder mittels Video, Ausweiserkennung und via Smartphone die „echte" Person verifizieren. „Aus diesen sogenannten phygitalen Identitfikationsverfahren haben wir uns in eine digitale Identifizierbarkeit hinentwickelt."

Die Vision der Zukunft muss sein, dass die Identität der Person on- und offline eindeutig, sicher und einfach feststellbar ist. Schließlich sind es die Online-Konsumenten gewöhnt, sich frei und userfreundlich in der Online-Welt zu bewegen.

Qual der Wahl

Dem Thema Sicherheit kommt entsprechend eine tragende Rolle zu. „Die Schwierigkeit ist die Qual der Auswahl. Die digitale Identität eindeutig festzustellen, bringt im Online-Business nicht nur mehr Sicherheit gegen Onlinebetrug. Vielmehr bedingen manche Geschäftsprozesse die rechtskonforme Identifizierung, beispielsweise beim Abschluss einer Online-Versicherung, eines Handyvertrags oder bei der Eröffnung eines Online-Bankkontos", erklärt Eder weiter. Es gibt allerdings nicht die eine Methode, die für alle Konsumenten die richtige ist. Dafür sind bereits zu viele unterschiedliche Verfahren im Umlauf und je nach Sicherheitsstufe mehr oder weniger sinnvoll bzw. notwendig.

Alles aus einer Hand

CRIF gibt dieser Vielfalt der Wege eine „Bühne" und vereint die verschiedensten Identifikations-Möglichkeiten auf einer Plattform. „Dieser Platform as a Service-Ansatz macht es den Händlern und Konsumenten maximal einfach und convenient: Als Identification Service Provider bietet CRIF über die Plattform die Vielzahl von Identifikations-Methoden an, die je nach Anforderung entlang der Customer Journey maßgeschneidert eingesetzt werden", so der Experte von CRIF. Somit bietet der Onlinehändler der Kundschaft die notwendige Auswahl und behält den Überblick über die Must-haves der Identifikationsbranche. Dies gilt über Landesgrenzen hinweg, im deutschsprachigen Raum und auch in Europa.

Partner von P19 Payment

Der Lösungsanbieter CRIF und die Payment-Plattform P19 haben eine Partnerschaft geschlossen. „Gemeinsam wird der Fokus auf einen aktiven Diskurs zur Zukunft des Risikomanagements im Zahlungsverkehr gelegt", so Birgit Kraft-Kinz, Co-Founder von P19 und CEO von Kraftkinz: „Risiko ist ein essenzielles Thema im Payment. Mit CRIF haben wir den richtigen Partner, um diese Themen in Österreich voranzutreiben." Eder kommentiert abschließend: „P19 ist ein wichtiges Payment-Netzwerk für Europa und Österreich. Wir freuen uns, mit unserer Erfahrung und Expertise im Risikomanagement und in der digitalen Identität im Zahlungsverkehr unseren Teil dazu beizutragen, gemeinsam die Entwicklung im Payment voranzutreiben und Neues in diesen Themengebieten anzudenken. Und das vor allem gemeinsam aus Österreich und Europa heraus."

> *Es gibt Tools, die einen physischen Abgleich digital abbilden oder mittels Video, Ausweiserkennung und Smartphone die ‚echte' Person verifizieren.*
>
> **Gerald S. Eder**
> *Director Digital Solutions bei CRIF*

Cash sicher verwalten

Ein geschlossener Bargeldkreislauf stärkt die Sicherheit im stationären Handel.

NEU-ISENBURG. Bargeld bleibt auf absehbare Zeit ein relevanter Faktor für den Handel, denn für viele Kunden ist Cash ein ungebrochen beliebtes Zahlungsmittel. Doch wo viel Bargeld im Umlauf ist, ergibt sich automatisch ein erhöhter Bedarf an Sicherheit. „Risiken bestehen an vielen Stellen im Retail: von der Extremsituation eines Überfalls auf Filialen oder Geldtransporter, über Ladendiebstahl bis hin zu – ganz alltäglich – unabsichtlichem Kassenschwund, der durch Fehler beim Zählen verursacht wird. So entwickeln Händler natürlich Sicherheitsbedenken im Umgang mit Cash", erklärt Oliver Kapahnke, Geschäftsführer, Glory Deutschland. „Genau an diesem Punkt setzt automatisiertes Bargeldmanagement an. Je seltener Bargeld bewegt wird und je weniger Personen damit in Berührung kommen, desto sicherer bleibt es."

Sicher automatisieren

Größtmögliche Sicherheit bieten Komplettsysteme, bestehend aus Hard- und Software, die alle Cash Touchpoints in Frontoffice und Kassenbüro miteinander vernetzen und zuvor isolierte Bargeldprozesse mit Geldtransport- und Bankpartnern zusammenführen. Mit den Recyclinglösungen CI-X aus der neuen Cashinfinity-Generation von Glory entsteht so ein komplett geschlossener Bargeldkreislauf. Das Cash wird aus dem tresorgesicherten System CI-10X vom Checkout geschützt ins Kassenbüro transferiert und dort automatisiert in der Backoffice-Lösung CI-100X weiterverarbeitet. Die nötigen Echtzeitgeräteinformationen liefert die angebundene Software CI-ServerX. Zu jedem Zeitpunkt vor dem Zugriff durch Unbefugte geschützt, stellt Bargeld dadurch nicht länger ein Sicherheitsrisiko dar.

© Glory

Glory hilft
„Risiken bestehen an vielen Stellen im Retail", weiß Glory Deutschland-Geschäftsführer Oliver Kapahnke.

„Professionalität der Angriffe steigt"

Karin Mair von Deloitte Österreich spricht über die aktuellen Risiken im Bereich Cybercrime.

WIEN. Das Beratungsunternehmen Deloitte erhebt in seinem Cyber Security Report jährlich gemeinsam mit dem Forschungsinstitut SORA den Status quo heimischer Betriebe beim Thema Cyber-Sicherheit. Für den vierten Report wurden 350 Mittel- und Großunternehmen in Österreich telefonisch befragt. Die Analyse zeigt: Die Zahl der Cyberangriffe hält sich im Vergleich zum Vorjahr zwar auf annähernd gleichem Niveau, gleichzeitig fällt es aber immer schwerer, die Attacken abzuwehren.

medianet: *Der Cyber Security Report des Vorjahres hat ergeben, dass knapp die Hälfte der österreichischen Unternehmen zumindest einmal pro Jahr von einem Cyber-Angriff betroffen ist und es massiven Aufholbedarf bei den Präventionsmaßnahmen gibt. Welche Entwicklungen gab es seither?*

Karin Mair: Die Bedrohungslage hat sich im letzten Jahr aufgrund der geopolitischen Ereignisse verschärft. Bei der Analyse der repräsentativen Umfrageergebnisse wird deutlich, dass sich Betriebe mit einer zunehmenden Professionalität der Angreifer auseinandersetzen müssen. Im Vergleich zum Vorjahr konnten 46 Prozent weniger Attacken durch technische Infrastrukturmaßnahmen verhindert und 30 Prozent weniger Daten nach einem Angriff wiederhergestellt werden. Das sind alarmierende Zahlen.

medianet: *Welche Maßnahmen setzen die österreichischen Unternehmen, um der verschärften Bedrohungslage zu begegnen?*
Mair: Die Unternehmen verfolgen nach wie vor eine Cyber-Security-Strategie, die überwiegend auf Prävention basiert. Angesichts der steigenden Professionalität der Angriffe sind klare Pläne, wie im Fall des Falles zu reagieren ist, erforderlich. Regelmäßige Tests und Evaluierungen dieser Pläne sind das Um und Auf.

© Deloitte/Feelimage

Karin Mair ist Managing Partner für Risk Advisory & Financial Advisory bei Deloitte Österreich.

medianet: *Welche Handlungsempfehlungen ergeben sich aus Ihrer Beratungspraxis?*
Mair: Angesichts der kritischen geopolitischen Lage spielt Risikomanagement eine zentrale Rolle für einen wirksamen Schutz. Auch wenn das einem Großteil der Unternehmen bewusst ist, plant rund ein Drittel keine Investitionen in die Implementierung oder die Verbesserung des Risikomanagements. Wir sehen hier Aufholbedarf. Außerdem wirkt sich das Fehlen von Talenten massiv auf die Cyber Security der Unternehmen aus. Eine sichere IT-Landschaft erfordert jedoch ausreichende, qualifizierte Personalressourcen. Wir empfehlen den Betrieben daher, die Entwicklung einer nachhaltigen Personalstrategie zu priorisieren, um für die Zukunft gerüstet zu sein.

Die Studie finden Sie unter: deloitte.at/cybersecurityreport

Mehr eCommerce, mehr Kriminalität

Betrügerische Handlungen treffen Online-Einzelhändler und Shop-Betreiber in einem massiven Ausmaß.

HAMBURG/WIEN. Der europäische Online-Handel verliert im Jahr 2022 3,1 Prozent seines Gesamtumsatzes durch Zahlungsbetrug. Diese Quote lag

> *Eine hohe Automatisierung ist aufgrund der Prozesskosten für manuelle Prüfungen wünschenswert, die manuelle Prüfung ist in Einzelfällen kaum verzichtbar.*
>
> **Risk.Ident GmbH**

© Tom Wilke

im Vergleich dazu im Jahr 2021 noch bei 3,0%. Risk.Ident GmbH geht davon aus, dass sich der Trend im Wachstumsmarkt Online-Betrug fortsetzt. Gründe sind die vermehrte Nachfrage nach Buy-Now-Pay-Later-Angeboten (BNPL) und die damit verbundenen Zahlungsausfälle.

Unterschätzte Problematik

Bei einem Online-Betrug geht es nicht einfach nur um Geld oder Waren – es ist ein Angriff, der mit großer Wahrscheinlichkeit wiederholt wird, wenn Betrüger Erfolg damit haben. Betrugsprävention schützt hingegen die Prozesse und die Gewinne vor gefälschten Identitäten, Identitätsübernahmen, Account Takeover, Friendly Fraud und allen anderen Betrugsmustern, die Risk.Ident GmbH über die Jahre begegnet sind. Online-Betrug wird allerdings teilweise unterschätzt, nicht beachtet und oft auch gar nicht wahrgenommen. Erst mit der Messung wird das bestehende Problem sichtbar. Die häufigsten Delikte in der D-A-CH-Region sind Account Takeover, Identitätsbetrug und der sogenannte Refund Fraud. Bei Ersterem übernehmen Betrüger einen bereits bestehenden Account von „Gutkunden" und versuchen das Vertrauen des Händlers in diesen Account auszunutzen. Identitätsbetrug liegt dann vor, wenn Betrüger sich als eine dritte Person ausgeben, um mit deren Identität vorhandene Bonitäts- und Betrugschecks zu umgehen und die Lieferung der Ware zu veranlassen. Im Falle des Refund Fraud versuchen Betrüger, bereits gelieferte Ware zu behalten, obwohl eine Retouren-Rückerstattung beim Händler ausgelöst wurde.

Optimale Balance

Ein häufiger Trugschluss ist, dass eine gute Betrugsprävention vollständig automatisiert sein muss. Eine hohe Automatisierung ist aufgrund der Prozesskosten für manuelle Prüfungen meist wünschenswert, die manuelle Prüfung ist in Einzelfällen und zur Aufdeckung neuer Muster jedoch kaum verzichtbar.

Hier geht es vor allem darum, Fehlentscheidungen zu vermeiden und gute Kunden zu halten – also direkt um Umsatz und Gewinn. Fakt ist: Bei einer guten Prävention kann mehr Kunden ein breiteres Spektrum an Zahlungs- und Lieferoptionen angeboten werden, was die Konversion erhöht. Eine sehr strikte Prävention erhöht wiederum die Menge an Kaufabbrüchen und Nachfragen. Dies kann vor allem im Outsourcing der Zugangssteuerung zum Problem werden. Eine gute Betrugsprävention steigert hingegen den Umsatz und reduziert das Risiko.

Risk.Ident GmbH wurde im Jahr 2012 als Tochterunternehmen der Otto Group gegründet und hat sich zum Marktführer im Bereich der Betrugsprävention in der D-A-CH-Region entwickelt.

Gefahr Ransomware

Axel Anderl und Nino Tlapak wissen, wie gefährlich Kryptoattacken auch für kleine Unternehmen sind. Bei LexisNexis haben sie ein Handbuch für die Praxis verfasst.

WIEN. Auf den ersten Blick ist die große Zeit von Kryptowährungen wie Bitcoin, Ethereum und Co. vorbei. Doch das ist sie nicht, vor allem nicht für Kriminelle. Axel Anderl und Nino Tlapak sind Rechtsanwälte bei Dorda Rechtsanwälte GmbH, halten Vorträge zum Thema Sicherheit und sind Herausgeber bzw. Autoren zahlreicher Fachpublikationen, u.a. dem aktuellen Werk „#Cybercrime" von LexisNexis. Im Interview erklären sie, warum die Gefahr derzeit groß wie nie ist, Opfer von Cyberkriminalität zu werden und was Kryptowährungen damit zu tun haben.

© LexisNexis Verlag

#Cybercrime
Das Buch ist für die Praxis, deckt nicht nur die relevanten Rechtsgebiete ab, sondern thematisiert auch technische und organisatorische Maßnahmen sowie Krisenkommunikation. Erschienen ist es bei LexisNexis, einem der führenden Anbieter für intelligente Rechtsinformation.

Betrug in großem Stil

Blockchain-basierte Währungen haben weiterhin einen großen „Vorteil": Sie sind anonym. Es würde für Kriminelle keinen Sinn machen, Lösegeld zu fordern, das auf ein klassisches Bankkonto überwiesen werden soll; die Geldübergabe im Koffer gibt es nur in Hollywood. „Kryptowährungen sind bei Tätern sehr beliebt und ein großes Problem", stellt Axel Anderl klar. Dabei gebe es zwei Tätigkeitsbereiche: Einerseits gehe es vor allem um Anlegerbetrug – beste Konditionen werden versprochen, das Geld bzw. das angekündigte Produkt oder Dienstleistung ist dann weg. Das kann alle Menschen betreffen.

Für Handelsunternehmen gilt andererseits: Ransomware-Attacken. Bei so einem Angriff verschafft sich die Malware Zugang zum Gerät: „Darüber schreiben wir das Buch: Die Angreifer dringen in das System ein und verschlüsseln Daten. Um sie freizubekommen, muss Lösegeld in Form von Kryptowährungen überwiesen werden. Das sind zum Teil horrende Beträge."

Milliarden, von allen geholt

Wie die beiden recherchiert haben, werden dabei Milliardenbeträge lukriert. Doch nicht nur von großen Unternehmen. Diese sind schon auch Opfer, aber sie haben ein hohes Sicherheitslevel. Tatsächlich sind es nicht selten staatlich finanzierte Hacker- bzw. Terrorgruppen, die so große Angriffe durchführen.

Relevanter für Kriminelle sind laut Nino Tlapak Klein- und Mittelbetriebe; sie sind „leichte" Angriffsziele, da die Sicherheitsmaßnahmen nicht so hoch sind. „Die Hacker fordern nicht immer Millionen, sondern oftmals bewusst einen vier-, fünf- oder sechsstelligen Betrag", erzählt er. „So kommt über viele Angriffe ebenfalls viel Geld zusammen, ohne komplexe Sicherheitsmaßnahmen durchbrechen zu müssen."

Tlapak kennt daneben Fälle, bei denen durch Passwort-Phishing Social Media-Profile von Einzelunternehmern lahmgelegt wurden: „Im Darknet kann ‚Cybercrime as a Service' als Toolpaket gekauft werden. So können auch kleinste Unternehmen standardisiert und ohne großen Aufwand angegriffen werden."

Wer sich „zu klein" für eine derartige Attacke fühlt, liegt eben falsch, vor allem, weil vielleicht gar nicht auffällt, wann und wie sich die Kriminellen Zugang verschaffen. Ein Phishing-Mail wird im Arbeitsstrudel schnell einmal geöffnet, vielleicht im August; erst im Weihnachtsgeschäft schlagen die Täter dann zu.

Einfache Maßnahmen helfen

Beide wissen: Man braucht kein Fort Knox, sondern einfachste Maßnahmen wie verschiedene, komplexere Passwörter oder regelmäßige Sicherheitsupdates. Beides einfache Maßnahmen, um die Cybersecurity zu erhöhen.

© Natascha Unkart & Isabelle Köhler (2)

Die Dorda-Rechtsanwälte Nino Tlapak (l.) und Axel Anderl kennen die Kryptogefahr.

HANDELS VERBAND

Bundesministerium Inneres
Bundeskriminalamt

GEMEINSAM.SICHER mit unserer Polizei

#sicherimhandel

Gemeinsam Sicher im Handel

Freier Eintritt!

SICHERHEITS-GIPFEL

10. MAI

ALBERT HALL, WIEN

2023