– Sonderveröffentlichung –

CYBERKRIMINALITÄT – SO KÖNNEN SIE SICH SCHÜTZEN

BETRUGSVERSUCH **IM INTERNET**

Der Faktor Mensch

Cyberkriminelle arbeiten mit immer ausgeklügelteren Techniken

Von Frank Beckenbach

Göttingen. Gerd L. (Name der Red. bekannt) ist 55 Jahre alt und nutzt seit mehr als 20 Jahren das Online-Banking-Angebot seiner Bank. Vor wenigen Wochen musste er feststellen, dass auf seinem Bankkonto plötzlich ein nicht unerheblicher Betrag fehlte. „Gut 18.000 Euro sind verschwunden, ich kann mir gar nicht vorstellen, was da passiert ist“, sagt der Inhaber eines kleinen mittelständischen Unternehmens. Er wurde natürlich umgehend bei seiner Bank vorstellig und fragte nach. Doch die Antwort, die er von den Finanzspezialisten bekam, gefiel ihm überhaupt nicht, denn seine Bank musste ihm mitteilen, dass er selbst für den erheblichen Verlust verantwortlich war. Was war geschehen? Moderne Zeiten, Online-Angebote, schnellste Überweisungsmöglichkeiten, einfach vom Computer oder dem Smartphone zu erledigen. All das sind Serviceangebote, die die Kunden der Banken gerne annehmen, nutzen und ganz schnell als selbstverständlich ansehen. Doch alles, was von den Banken ausgeht, das ist zu 99,9 Prozent sicher. Die Verfahren, ob pushTAN oder Generator – also alle Maßnahmen, die derzeit angewandt werden – sichern die Online-Bankgeschäfte zeitgemäß ab. Wenn da nicht der Faktor Mensch ins Spiel kommen würde.

„In den vergangenen Monaten haben wir eine Zunahme der digitalen Betrugsversuche wahrgenommen. Bei diesen versuchen die Täter an die persönlichen Daten, wie zum Beispiel die Kennwörter, unserer Kundinnen und Kunden zu kommen“, sagt Ines Dietze, neue Vorstandsvorsitzende der Sparkasse Göttingen. „Es liegt in unser aller Verantwortung, Aufforderungen, wie beispielsweise auf einen Link zu klicken oder ein Passwort einzugeben, kritisch zu hinterfragen und im Zweifel die eigene Kundenberaterin oder den eigenen Kundenberater zu kontaktieren.“ Jeder Einzelne müsse darauf achten, wie er sich im Internet bewege und welche Daten er teilt. „Wir als Sparkasse Göttingen leisten ein hohes Maß an Aufklärungsarbeit, wie unsere Kunden sicher im Internet unterwegs sein können. Zudem bietet unsere Internet-Filiale ein hohes Maß an Sicherheit für das Online-Banking – aber wir sind maßgeblich auf die wachsamen Handlungen der Kunden angewiesen: Die besten Sicherheitsmaßnahmen nützen nämlich nichts, wenn die Zugangsdaten in die falschen Hände gelangen.“

Fast 1.500 Fälle von „Cybercrime“ wurden im Bereich der Polizeiinspektion Göttingen aktuell ermittelt. Über 100 Fälle mehr als im Vorjahr. Es wurden Daten ausgespäht, abgefangen, es gab Datenhehlerei, Datenveränderungen, Computersabotagen und Erpressungen mit Ransomware.

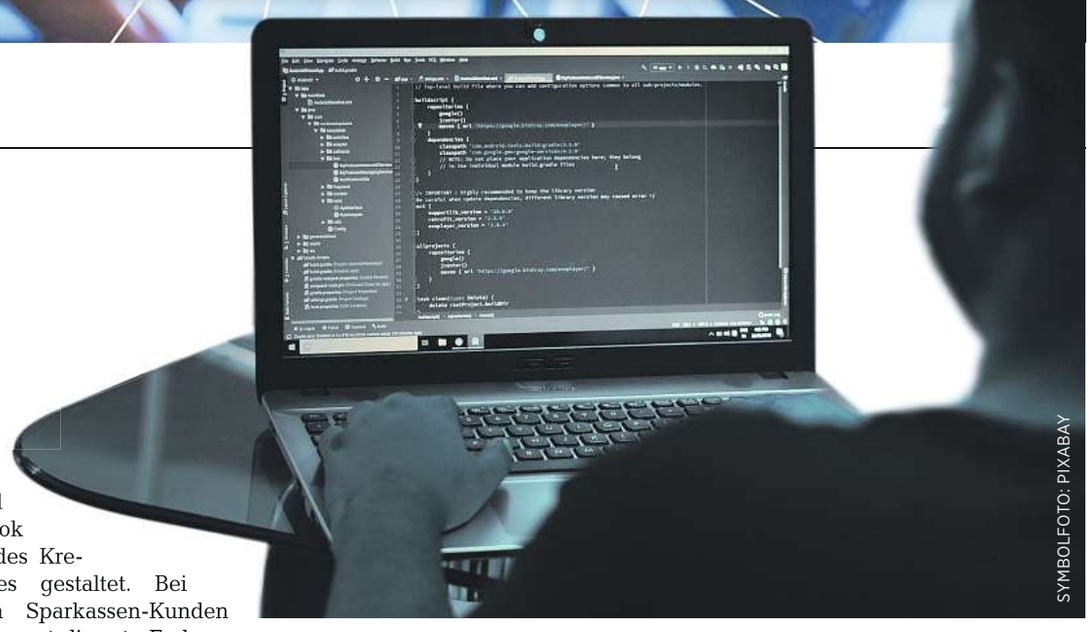
Das bedeutet, viele Cyberkriminelle sind am Werk, aber denen sollte man es so schwer wie möglich machen: Denn es sind die kleinen Fehlverhalten und Unachtsamkeiten, die allergrößten Schaden anrichten können.

Was bei Gerd L. passiert war, ist exemplarisch nachvollziehbar. Es begann ganz harmlos. Durch das einfache Öffnen von unbekannten Mailanhängen bekommen die Cybergauner einen ersten Zugang zum Computersystem ihres Opfers. Viele Mails landen gleich im Spam-Ordner, sind also gleich Müll. Das kennt heutzutage jeder, der einen E-Mail-Account besitzt. Es kommen aber immer mehr Mails daher, die scheinbar doch wichtig sind. Selbstverständlich interessiert es, wann das lang erwartete Paket ankommt oder warum es nicht zugestellt werden konnte. Vielleicht sagt eine Mail auch, dass ein Account gesperrt wurde, so bei Gerd L.. Der Computernutzer schaut nach und schon haben die Cyberkriminellen die erste Aufmerksamkeit bekommen. Doch all das ist eine Fakemail, ein Schwindel, nur eine Gelegenheit, um an Daten von gutgläubigen Computernutzern zu gelangen. Die Cybergauner nutzen hier einfach die große Wahrscheinlichkeit, dass der Adressat tatsächlich ein Paket erwartet oder einen Amazon-Account hat.

Hat der User solch‘ eine „gefakte“ Seite aufgerufen, geht es, auch aus Sicht des Öffnenden, leider relativ harmlos weiter: Es werden jetzt normalerweise Daten wie Vor- und Nachname, Adresse, Telefonnummer, E-Mailadresse abgefragt. Wenn es den Betrügern gelingt, sogar schon die IBAN, also die Internationale Bank Account Number, zu ergattern, ist das fast schon der Sechser im Lotto.

Hat der Kunde diese Daten weitergegeben, dann passiert erst einmal eine Zeit lang nichts. Zudem nutzen die Kriminellen auch gehackte Konten von Unternehmen, um an weitere Informationen heranzukommen. Gerd L. bemerkte das erst einmal nicht.

Irgendwann erhält der Bankkunde dann eine sehr viel spezifischere Mail. Seine Bank ist nun den Tätern bekannt und sie sind im Besitz einer Kontoverbindung. Zudem wird diese Mail im „Look & Feel“ des Kreditinstitutes gestaltet. Bei Mails an Sparkassen-Kunden wird bevorzugt die rote Farbgebung verwendet, bei den Volksbanken die blaue. Inhaltlich sind zudem Informationen von den Internetseiten der Bank hübsch für diese Mail aufbereitet – beispielsweise, ganz aktuell, die Verhaltens-Vorgaben für Covid-19. In jedem Fall wird dem Mailadressat sehr professionell vorgegaukelt, dass es sich um eine „echte“ Mail handelt.



SYMBOLFOTO: PIXABAY

Bei diesen Mails gibt es immer einen Link, auf den geklickt werden muss. Manchmal ist sogar die gesamte Mail dieser Link. Über diesen Link werden die Kunden nun aufgefordert, sich beim Online-Banking einzuloggen. Tut das ein Bankkunde im guten Glauben, dann ist der nächste Schritt schon vorprogrammiert.

Denn der Kunde wird nun geschickt weiter manipuliert. Ziel ist es, auch noch an die TAN heranzukommen, um dann tatsächlich Geld abheben zu können.

In einer nächsten Mail, der nächste Schritt, werden die Bankkunden zur Zusammenarbeit aufgerufen, wer gut mitarbeitet, dem werden Bonifikationen, wie kostenlose Kontoführung oder kostenfreie Bargeldabhebung im Ausland angeboten. Kunden, die zögern, wird die Sperrung ihres Kontos angedroht. Es wird hier also mit Zuckerbrot und Peitsche von Seiten der Gauner gearbeitet.

Haben die Cybergangster den Bankkunden an der Angel, geben sie sich nicht mit wenig zufrieden. Sie fragen auch nach Geburtsdatum und Kartendaten, die können sie gut für beispielsweise eine Limiterhöhung gebrauchen.

Dann wird auch noch der Anruf eines Bank-Mitarbeiters angekündigt, als weitere „vertrauensbildende Maßnahme“ und gleichzeitig eine erfundene „Legitimations-PIN“ angezeigt. Mit dieser wird sich der Anrufer, der natürlich überhaupt nichts mit der Bank zu tun hat, dann legitimieren und der Angerufene denkt: „Das muss ja meine Bank sein, der Anrufer hat sich ja legitimiert.“

Die Cybergauner überprüfen in der Zeit die Konten ihres potenziellen Opfers. Ist genügend Geld vorhanden? Denn die Täter können sich ja längst auf die Kundenkonten des potenziellen Opfers einwählen, Kontostände einsehen, ebenso den Kreditrahmen, die Online-Banking-Limite und sie wissen nun auch, wer der persönliche Berater des Kunden ist.

Lohnt sich der Angriff auf das Konto, dann wird der Kunde angerufen. Auch hier ist der Angriff sehr ausgeklügelt, denn der Gauner, der reines Hochdeutsch spricht, hat umfassendes Wissen erworben und baut jetzt Vertrauen zum Opfer auf. Sogar die Telefonnummer, über die er anruft, ist als die Nummer der Bank des Kundens zu identifizieren – diese Anzeige ist natürlich manipuliert worden.

Zu diesem Punkt weiß der Cybergauner zwar schon sehr viel über den Kunden, eine Transaktion kann er aber (noch) nicht vollziehen. Aber er hat das Vertrauen des Bankkunden erschlichen. Autorisiert der Kunde eine Transaktion via TAN, die er an den Täter weitergibt oder gibt er die Transaktion via pushTAN frei, dann ist sein Geld in aller Regel verloren. Wird ein Kunde nun doch noch misstrauisch, werden die Bedenken durch den Täter zerstreut – es handele sich beispielsweise doch nur um eine Testüberweisung.

Die Täter veranlassen, wenn sie in den Besitz aller wichtigen Zugangsdaten gelangt sind, die Zurücksetzung des pushTAN-Verfahrens oder die Umstellung auf dieses. Dies geschieht per SMS auf eine vorhandene Mobilfunknummer mit dem Hinweis, dass die URL zur Registrierung nicht weitergegeben werden darf. Leider geschieht dies häufig aber doch. Dann benötigen die Täter den Kunden nicht mehr, haben den Zugriff auf das Konto und können Transaktionen freigeben. Zudem ändern die Täter auch schnell die PIN, sodass für den Bankkunden die getätigten Bankverfügungen gar nicht mehr nachzuvollziehen sind.

Schnell entstehen durch diese Aneinanderreihung von Leichtfertigkeiten Schäden im fünf- bis sechsstelligen Bereich, denn die Täter räumen die Konten sehr effektiv leer, erhöhen so weit wie möglich die Tageslimite und auch die Sparbücher bleiben nicht verschont.

Die Täter nutzen bevorzugt Echtzeitüberweisungen, da dort die Gelder innerhalb von 20 Sekunden rund um die Uhr beim Empfängerinstitut, zumeist Direktbanken, sind.

Was tun, wenn das Kind schon in den sprichwörtlichen Brunnen gefallen ist? Die Spezialisten der Sparkassen Göttingen und Duderstadt, der VR-Banken Mitte und Südniedersachsen, der Volksbank Kassel Göttingen sowie der Vorsitzende des Vereins für Cybersicherheit e.V. geben nun wertvolle Tipps rund um das Thema Cyberkriminalität.

FLORIAN HARTLEIB

VR-BANK MITTE

„Die Entwicklung der Nutzerzahlen und die entstehenden Betrugsfälle machen unsere Präventionsarbeit zu einer sehr wichtigen Aufgabe“, sagt Florian Hartleib, Prokurist der VR-Bank Mitte. Daher sei auch der Umgang im Betrugsfall ein wichtiger Bestandteil der Präventionsarbeit. „Dafür haben wir eine digitale Checkliste erstellt, die unseren Mitglieder und Kunden in der dann vorhandenen Stresssituation Orientierung darüber bietet, was zuerst und was zuletzt gemacht werden muss“, sagt Hartleib. „In den meisten Fällen geben die Nutzer sensible Daten wie PIN und TAN an die Betrüger weiter und diese Tatsache ist nicht versicherbar. Daher unsere Bitte: Geben Sie niemals sensible Daten an Fremde heraus und achten Sie darauf, wo Sie diese sensiblen Daten eingeben.“

JAN DANIEL BREMER

VR-BANK IN SÜDNIEDERSACHSEN

„Sperren Sie umgehend das Online Banking bei Ihrer Bank – entweder über unsere Telefonfiliale 05502 / 910 444 oder über den 24/7 Sperr-Notruf 116 116“, sagt Jan Daniel Bremer, Business Administrator der VR-Bank Südniedersachsen. „Denken Sie auch an andere Personen, bei denen Sie bevollmächtigt sind, auch diese sollten umgehend ihre Kontoumsätze überprüfen“, sagt Bremer. „Bringen Sie den Fall bei der Polizei zur Anzeige und wenden Sie sich an einen PC-Spezialisten, wenn Ihr Rechner oder Smartphone zum Angriffsziel von Hackern geworden ist.“

DANIEL ZÖPFGEN

SPARKASSE DUDERSTADT

„Sollte man feststellen, dass eine betrügerische Überweisung ausgeführt wurde, am besten sofort das Online-Banking sperren und persönlich mit der Sparkasse in Verbindung setzen“, sagt auch Daniel Zöpfgen, Fachberater für Giro- und Zahlungsverkehr der Sparkasse Duderstadt. Das funktioniere bequem über die Internetseite der Sparkasse. Auch über den 24h-Sperrnotruf 116 116 ist eine Sperrung des Online-Banking Zugangs telefonisch möglich. Es gäbe Versicherungen, die gegen die Cyberangriffe versichern. Welche Bedingungen erfüllt sein müssten, damit solche Schäden reguliert werden können, sei mit der jeweiligen Versicherungsgesellschaft zu klären. Zöpfgen empfiehlt hier eine individuelle Beratung.

MARCEL WAGENER

SPARKASSE GÖTTINGEN

„Als erstes sollten die Kunden versuchen, Kontakt mit ihrem Kundenberater oder ihrer Kundenberaterin aufzunehmen“, sagt Marcel Wagener, Abteilungsleiter für Payment-Themen bei der Sparkasse Göttingen. „Alternativ steht ihnen die kostenlose Sperrhotline 116 116 rund um die Uhr zur Verfügung.“ Für die Wiederaufnahme der Online-Banking-Aktivitäten sollten anschließend unbedingt neue Anmeldenamen und Kennwörter verwenden werden. Es gibt spezielle Versicherungen, so Wagener, mit denen sich die Kunden gegen Risiken und Fehler im digitalen Lebensalltag absichern können. „Ähnlich wie bei einer Haftpflichtversicherung empfehlen wir nicht nur unseren gewerblichen, sondern auch allen privaten Kunden eine entsprechende Ergänzung in Form einer Cyberversicherung, da diese unter anderem auch bei Eigenschäden leistet.“ Unerlässlich sei allerdings, dass die Kunden ebenfalls ihren Beitrag zur Sicherheit ihrer Onlinegeschäfte in Form von regelmäßigen Sicherheitsupdates und anderer Schutzvorkehrungen leisten.“

ANNETTE BÖHLE

VOLKSBANK KASSEL GÖTTINGEN

„Häufig kommen den Kunden die Zweifel, ob sie gerade richtig gehandelt haben, unmittelbar nach der Eingabe ihrer Daten auf Fake-Seiten oder auf Links von Phishingmails“, sagt Annette Böhle, Abteilungsleiterin Zahlungsverkehr der Volksbank Kassel Göttingen. „Dann sollte umgehend die Bank kontaktiert werden, um den Online-Zugang zu sperren. Dies kann telefonisch über die Sperrhotline 116116, über unser KundenServiceCenter oder direkt im Online-Banking erfolgen. Sofern ein Schaden entstanden ist, ist Anzeige zu erstatten.“ Leider seien die Schäden im Online-Banking in den meisten Fällen in der leichtfertigen Eingabe der Daten durch den Kunden selbst begründet, was einer Verletzung der Sorgfaltspflichten gleich kommt“, sagt Böhle. Einige Versicherungen böten, im Rahmen von Zusatzpaketen in der Hausratversicherung, einen Versicherungsschutz für Internetschäden an.

UWE LÜHRIG

VEREIN FÜR CYBERSICHERHEIT NIEDERSACHSEN

„Innerhalb Deutschlands und einigen Teilen Europas ist die Nachverfolgung von Geldtransfers möglich. Das wissen aber auch die Täter“, sagt Uwe Lührig, 1. Vorsitzender des Vereins für Cyber-Sicherheit Niedersachsen e.V.. „Deshalb wird das Geld unverzüglich auf Konten, die sich außerhalb Europas befinden, transferiert. Hier sind dann für die weiteren Ermittlungen umfangreiche und lang andauernde Rechtshilfeersuchen erforderlich. In der Zwischenzeit haben die Täter das Geld längst abgehoben und das Konto aufgelöst.“ Dass die Täter bei der Kontoeinrichtung in der Regel ebenfalls mit falschen Identitäten arbeiten, müsse an dieser Stelle nicht weiter erläutert werden, sagt Lührig. Der Verein für Cyber-Sicherheit Niedersachsen e.V. (VCS) sei mittlerweile Teilnehmer in der „Allianz für Cyber-Sicherheit“ und Mitglied im Cyber-Sicherheitsrat Deutschland e.V.. „Wir geben regelmäßig Präventions- und Warnhinweise des BKA (Bundeskriminalamt) und des BSI (Bundesamt für Sicherheit in der Informationstechnik) an unsere Mitglieder (mittelständische Unternehmen, Kommunen und auch Privatpersonen) weiter und sensibilisieren zum Thema Cybersicherheit. Das kann auf Wunsch des jeweiligen Unternehmens auch vor Ort geschehen“, sagt Lührig. Für das Jahr 2022 seien vier bis fünf Informationsveranstaltungen zum Thema Cybersicherheit – gemeinsam mit Kooperationspartnern – geplant.