RUNDSCHAU FÜR MERZIG-WADERN

MIT BECKINGEN, LOSHEIM AM SEE, MERZIG, METTLACH, PERL, WADERN UND WEISKIRCHEN

BECKINGEN
Das Juz hat sein 20-jähriges Bestehen gefeiert. Seite C 2

HILBRINGEN/LOSHEIM
Urkunden für Ehrenamtler im Fußball Seite C 3

Wie Datendiebe ihre Opfer abfischen

Sparkasse Merzig-Wadern warnt Nutzer von Online-Banking vor betrügerischen Maschen per Telefon, E-Mail oder SMS.

VON CHRISTIAN BECKINGER

MERZIG Online-Banking wird immer beliebter. Mehr und mehr Bankkunden entscheiden sich dafür, ihre Bankgeschäfte vorzugsweise am PC oder noch simpler mit dem Smartphone oder Tablet zu erledigen. Das geht rund um die Uhr, funktioniert ohne Zweigstelle, die aufgesucht werden muss, und ist überdies in der Regel kostengünstiger als die klassische Art der Kontoführung. Bei der Sparkasse Merzig-Wadern beispielsweise nutzen nach eigenen Angaben gut zwei Drittel der Privatkunden bereits die Möglichkeiten des Online-Bankings, bei den Geschäftskunden liegt die Nutzer-Quote noch höher, bei über 80 Prozent.

Aber der Vormarsch des Digitalen hat auch Schattenseiten: Denn dadurch werden die Nutzerdaten der Bankkunden immer wertvoller für Menschen, die nichts Gutes im Schilde führen. Ist jemand erst einmal im Besitz von Kontozugangsdaten, besteht das Risiko, dass er sich Zugriff auf die Gelder beschafft, die auf diesen Konten deponiert sind. Der Versuch, an diese Nutzerdaten heranzukommen, wird als „Phishing“ bezeichnet, abgeleitet vom englischen Wort für „fischen“.

Die Maschen, mit denen Kriminelle versuchen, an die Bankdaten von Online-Banking-Nutzern heranzukommen, sind ebenso vielfältig wie raffiniert, wie Frank Jakobs, Vorstandschef der Sparkasse Merzig-Wadern, am Beispiel gefälschter E-Mails einräumt: „Diese Sachen sehen mitunter extrem vertrauenswürdig aus, man fällt wirklich gerne darauf herein.“ Für Michael Gleissner, Leiter der Abteilung „Medialer Vertrieb“ bei der Sparkasse, sind diese Betrugsmaschen eine permanente Herausforderung. Denn trotz diverser Sicherheitsmechanismen, die die Sparkassen (und die meisten anderen Banken ebenso) mittlerweile in ihre Online-Banking-Prozeduren eingebaut haben (siehe separater Text), gelingt es Bösewichten immer wieder, sich die Zugangsdaten von Kunden zu erschleichen und mitunter auch die Sicherheitsbarrieren zu umgehen.

„Wir haben im Jahr 2021 insgesamt 16 Betrugsversuche registriert. Davon konnten wir in zehn Fällen einen Schaden für den Kunden noch vermeiden, in sechs Fällen ist allerdings tatsächlich ein Schaden entstanden“, listet Gleissner auf. Gerade in jüngster Zeit beobachte man eine Zunahme von betrügerischen Anrufen, dem so genannten Call Spoofing: Der Anrufer gibt sich dabei als Mitarbeiter der Sparkasse oder Bank aus und versucht, sein Opfer so zur Herausgabe von geheimen Informationen und zur Installation von Schad-Software auf PCs zu verleiten. Besonders dreist: Häufig manipulieren die Täter die Telefonnummer, die auf dem Display des Smartphones oder Telefons angezeigt wird, um die Richtigkeit des Anrufs vorzutäuschen. Anrufe erfolgen nach den Worten von Gleissner zudem oft außerhalb der normalen Öffnungszeiten der Sparkasse, um den Opfern die Möglichkeit zu nehmen, sich bei der Sparkasse rückzuversichern. Im Verlauf des Telefongesprächs versuchen die Online-Kriminellen, Kunden zur Herausgabe von Zugangsdaten zum Online-Banking zu überreden und gegebenenfalls eine oder mehrere Transaktionsummern (TAN) zu nennen, die dann aufs Smartphone geschickt werden. Oft wird behauptet, diese TANs seien für notwendige Rücküberweisungen oder bestimmte technische Prüfungen und die Einführung eines neuen Sicherheitssystems erforderlich. „Das stimmt natürlich nicht. Unsere Mitarbeiterinnen und Mitarbeiter werden niemals am Telefon nach Online-Banking-Zugangsdaten oder TANs fragen“, betont Gleissner.

Eine sehr verbreitete Masche sind auch täuschend echt aussehende E-Mails, die vermeintlich von der eigenen Bank geschickt worden sind. Und in denen die Täter massiven Druck auf ihre Opfer ausüben, wie Michael Gleissner erläutert: „‚Ihr Konto wurde vorübergehend gesperrt‘ oder ‚Sie müssen Ihre Zugangsdaten aktualisieren‘ – so oder ähnlich lauten meist die Betreffzeilen der E-Mails, die den Kunden beim Phishing die Passwörter abgreifen wollen.“ Die dringend klingende Mail lockt den Empfänger der Mail über einen Link auf täuschend echt aussehende Kopien der originalen Internetseite. Auf den manipulierten Seiten sollen Kunden dann beispielsweise Geheimzahl (PIN) oder Einmalpasswort (TAN) eingeben. Gleissner: „Vermeintlich, um das Konto wieder freizuschalten. Stattdessen erbeuten die Datenfischer hochsensible Informationen.“

Das Phishing per Mail ist die gängigste Variante, nach Gleissners Worten erfolgen drei Viertel aller Datenklau-Versuche auf diesem Weg. Eine andere Masche ist das Phishing per SMS, das so genannte Smishing: Als Bank getarnt, fordert eine Betrügerin oder ein Betrüger Kunden in einer SMS dazu auf, persönliche Daten zu aktualisieren oder etwas in einem persönlichen Account zu überprüfen. Michael Gleissner: „Meist ist die Nachricht mit einer Drohung verbunden – zum Beispiel, dass bei Nichtbefolgen das Konto gesperrt wird.“ Die SMS enthalte oft einen Link zu einer Fake-Website, auf der man die Login-Daten eingeben soll. Dadurch kann der Täter die Kombination aus Nutzernamen und Passwort abgreifen.

Wie man sich hiergegen wappnen kann, erklärt Gleissner: „Am wichtigsten sind gesundes Misstrauen und Aufmerksamkeit. In manchen Fällen sticht einem die Phishing-Nachricht direkt ins Auge, in anderen müssen Kunden etwas genauer hinsehen.“ So sollten Kunden die per Mail oder SMS eingegangene Nachricht auf Rechtschreibfehler prüfen – ein gutes Indiz dafür, dass die Zusendung in betrügerischer Absicht erfolgt ist. Auch hinsichtlich der gewählten Ansprache können einem Ungereimtheiten leicht ins Auge fallen. Bei E-Mails sollte man genauestens auf den Absender (also die Mailadresse) und insbesondere die Absender-Endung achten. Sinnvoll ist auch, den angeblichen Absender anzuschreiben und nachzufragen. Im Falle von eingehenden SMS sollte man die Mobilfunknummer durch Rückruf überprüfen.

Daneben ist auch Vorsicht geboten beim Herunterladen von Programmen aus dem Internet auf den PC oder dem Installieren von Apps auf dem Smartphone: Dabei können ungewollt so genannte Spyware oder Trojaner auf dem Gerät installiert werden. Michael Gleissner erläutert: „Wie ihr griechisches Vorbild schleusen Trojaner unbemerkt Spionageprogramme auf Computern oder Smartphones ein, ähnlich wie Viren.“ Deren Zweck: zum Beispiel Kontodaten und Passwörter klauen. Bei Spyware handele es sich um Software, die den Computer oder das Smartphone ausspioniert. Gleissner: „Spyware mogelt sich meist unerkannt im Schlepptau harmloser Software auf einen Computer. Zum Beispiel über Gratis-Software oder Apps, die eigentlich das Leben erleichtern sollen.“ Sie stiehlt Daten und überträgt diese an Fremde. Hier sollten die Nutzer darauf achten, dass ihre digitalen Endgeräte einen aktuellen Virenschutz nutzen und außerdem sehr vorsichtig beim Herunterladen von neuen Programmen oder Apps sein.

Kontodaten am Haken: Immer wieder versuchen Kriminelle, von Nutzern des Online-Bankings sensible Informationen zu ergaunern. FOTO: ANDREA WARNECKE/DPA

INFO

Zehn Tipps für mehr Sicherheit

Zehn wichtige Tipps der Sparkassen-Experten für einen sicheren Umgang mit Online-Banking und die Abwehr von Phishing-Attacken:

(1) Gehen Sie sicher, dass Sie nur Software von sicheren und vertrauenswürdigen Internetseiten herunterladen. (2) Aktualisieren Sie regelmäßig Ihr Betriebssystem, den Browser und Virenscanner. (3) Erledigen Sie Bankgeschäfte oder Online-Einkäufe nie über ein fremdes Wlan. (4) Hinterlegen Sie keine persönlichen Zugangsdaten auf fremden Portalen, geben diese auch nicht an Dritte weiter. (5) Achten Sie darauf, dass Sie Online-Geschäfte nur über eine verschlüsselte Verbindung tätigen. (6) Für Online-Banking oder einen Einkauf im Internet tippen Sie die Internet-Adresse direkt im Adressfeld ein und vermeiden Sie es, Internet-Suchmaschinen zu nutzen. (7) Öffnen Sie keine Dateianhänge in E-Mails von unbekannten Absendern. (8) Folgen Sie nie Aufforderungen, die Sie per E-Mail oder Telefon erhalten, Zahlungsaufträge zu bestätigen. (9) Achten Sie auf ungewöhnliche Anzeigen und Vorgänge im Online-Banking. (10) Geben Sie nur eine TAN ein, wenn Sie vorher einen Auftrag erteilt haben.

Die Zugangsdaten allein reichen nicht, um ans Geld zu kommen

MERZIG (cbe) Um zu vermeiden, dass ihre Online-Banking-Kunden Opfer von betrügerischen Maschen werden, setzen Banken und Sparkassen auf mehrstufige Sicherheitssysteme. Diese sollen es Kriminellen erschweren, selbst mit ergaunerten Zugangsdaten an Geld von Bankkonten heranzukommen.

Der bloße digitale Zugang allein zum Bankkonto reicht nicht aus, um beispielsweise Geld von dort an ein anderes Konto zu transferieren. Hier ist die so genannte Zwei-Faktor-Authentifizierung zwischengeschaltet: Neben der Eingabe der individuellen Zugangsdaten muss der Kunde zum Ausführen einer Konto-Transaktion zum Beispiel noch einen mehrstelligen Code (TAN) eingeben. Diesen kann der Kunde selbst erzeugen, mittels eines so genannten TAN-Generators, den er mit seiner Bankkarte aktiviert. Die so erzeugte TAN ist nur für einen genau definierten Vorgang gültig und muss innerhalb einer bestimmten Frist genutzt werden.

Michael Gleissner, Leiter Medialer Vertrieb FOTO: MANFRED MÜLLER/SPARKASSE

Daneben gibt es bei den Sparkassen auch das sogenannte PushTAN-Verfahren, das vor allem von Kunden genutzt wird, die ihr Online-Banking auf Mobilfunk-Geräten wie Smartphone oder Tablet erledigen. Hierzu benötigen sie die kostenfreie App S-pushTAN, die wiederum durch ein eigenes Passwort oder eine biometrische Identifizierung (etwa den Fingerabdruck) entsperrt werden muss. In dieser App muss der Kunde einen Auftrag, den er im Online-Banking erteilt hat, dann nochmals freigeben. Bei beiden Verfahren werden der Betrag, um den es geht, sowie die IBAN des Empfängerkontos zu Kontrollzwecken nochmals angezeigt.

Die Sparkasse Merzig-Wadern legt nach Worten von Michael Gleissner großen Wert darauf, dass sie selbst nicht zum Ziel von Hackern wird, die sich Zugriff auf Kundendaten verschaffen. „Die Kundendaten sind bei uns immer sicher aufgehoben und zugriffsgeschützt“, betont er. Eine sichere Datenübertragung bei allen Transaktionen sei durch moderne Verschlüsselungstechniken ebenso gewährleistet wie die sichere Speicherung aller Kundendaten ausschließlich auf den deutschen Servern der Sparkassen-Organisation. Es gebe keine Datenablage in Cloud-Speichern (also über Webseiten) oder auf Auslandsservern.

Produktion dieser Seite:
Alexander Manderscheid
Astrid Dörr