bankenverband

Themenbeitrag
Lexikon Cyberkriminalität

1. Oktober 2020

Tagtäglich werden viele Internet-Nutzer Opfer von Online-Betrug. Aber welche Angriffsformen gibt es, und wie kann man sich davor schützen?

Wir haben hier typische Cyber-Attacken und Tipps zur Abwehr und Vorsorge gegen Onlinekriminalität zusammengestellt. Manche Angriffe, wie zum Beispiel das Phishing, sind seit Jahren bekannt, werden aber – auch durch die sich beschleunigende Digitalisierung aller Lebensbereiche – beständig verändert und ausgefeilter. Deshalb ist es wichtig, sich immer wieder über die grundlegenden Maßnahmen zum Schutz vor Cyberkriminalität zu informieren.

Der Europäische Aktionsmonat zur Cybersicherheit (European Security Month, ECSM) legt 2020 einen besonderen Fokus auf den Schutz vor Onlinebetrug. Der Bankenverband unterstützt den ECSM auch in diesem Jahr wieder mit einer digitalen Informationskampagne.

A: Account Takeover

Ein Account Takeover (Deutsch: Kontoübernahme) ist ein Identitätsdiebstahl und -betrug, bei dem sich ein Dritter die Zugangsdaten z. B. eines fremden Mail-Accounts verschafft, um diesen für kriminelle Zwecke zu missbrauchen. Dazu gehören die Änderung von persönlichen Daten wie beispielsweise das Passwort, Versand von Phishing-Mails und der Diebstahl sensibler Daten.

Tipps:

- Wählen Sie ein starkes Passwort: Verwenden Sie Groß- und Kleinbuchstaben, Sonderzeichen und keine persönlichen Angaben wie Geburtsdaten, Namen oder ähnliches.
- Überprüfen Sie Ihre persönlichen Online-Accounts regelmäßig. Die Zugangsdaten gehen nur Sie etwas an, geben Sie diese nicht an Dritte weiter. Auch in die sozialen Medien gehören Ihre persönlichen Daten nicht.
- Informieren Sie bei Unregelmäßigkeiten im Zusammenhang mit dem Bankkonto schnellstmöglich die Bank und kontaktieren Sie die Polizei, wenn Sie einen Betrugsverdacht haben.
- Zusätzlichen Schutz bietet eine Zwei-Faktor-Authentifizierung. Die funktioniert so: Der Nutzer gibt zum Beispiel neben dem Passwort noch eine Transaktionsnummer ein, um sich anzumelden. Alternativ wird die Beantwortung einer Sicherheitsfrage bei fehlerhaften Anmeldeversuchen gefordert. Der Account wird zudem bei zu vielen fehlerhaften Anmeldeversuchen gesperrt.

Weitere Informationen:

Flyer „Wie schütze ich mich vor Phishing?“

Blog „Sicherheitstipps fürs Onlinebanking“

B: Botnetze

Ein Botnetz ist ein Netzwerk von Computern, das von einem Server gesteuert wird. Die Computer werden mit Schadprogrammen (Trojanern) infiziert und können dann ohne Wissen des Besitzers kontrolliert und zu kriminellen Zwecken missbraucht werden, beispielsweise zum Versand von Spam-Mails oder zur Durchführung von Denial-of-Service-(DoS)-Attacken.

Tipps:

- Der beste Schutz, um nicht unbemerkt Teil eines Botnetzes von Cyberkriminellen zu werden, sind ein aktueller Virenscanner, eine aktuelle Firewall und aktuelle Browser. Wichtig: Auch deren Aktualisierungen sollten zeitnah heruntergeladen werden.
- Ist der PC erstmal befallen und Teil eines Botnetzes, kann ein Laie das kaum erkennen. Ein Hinweis kann aber sein, dass der PC bei der Internet-Nutzung ungewöhnlich langsam ist.

C: CEO-Fraud / Chef-Betrug

CEO ist die Abkürzung für Chief Executive Officer, also Geschäftsführer. Fraud ist das englische Wort für Betrug. Beim CEO-Fraud haben es Kriminelle auf das Geld von Firmen abgesehen. Sie spionieren ein Unternehmen über einen langen Zeitraum aus, bis sie mit den internen Abläufen vertraut sind. Dann schlagen sie zu: Sie geben sich als vermeintlicher Chef des Unternehmens aus und bringen ahnungslose Mitarbeiter dazu, vertrauliche Finanztransaktionen durchzuführen. Die Betrüger passen die Gründe dem Unternehmen an, nehmen beispielsweise Bezug auf konkrete Geschäfte oder geplante Investitionen. Es gibt unter anderem Fälle, in denen die Bankverbindung des Empfängers durch die des Täters ersetzt wird (Mandate-Fraud). Per E-Mail wird eine angeblich neue Bankverbindung eines Geschäftspartner bekannt gegeben.

Tipps:

- Prüfen mit gesundem Menschenverstand: Als Mitarbeiter eines Unternehmens - gerade in der Buchhaltung oder ähnlichen Abteilungen - sollte man besonders wachsam sein. Beim Chef-Betrug werden die betroffenen Unternehmen oftmals über einen langen Zeitraum ausspioniert, so dass viele interne Informationen bekannt sind. So kann ein vermeintlich vertraulicher und sehr eiliger Zahlungsauftrag vom Chef mit vielen richtigen Informationen gespickt sein. Selbst bei Anrufen mit der vermeintlich bekannten Stimme muss man skeptisch sein: Mittels Sprachcomputer können Stimmen imitiert werden.
- Fragen Sie nach: Im Zweifel muss man sich trauen, bei ungewöhnlichen Geschäftsvorfällen nachzuhaken. Das Bauchgefühl kann stimmen! Ist eine Zahlung erstmal ausge-

löst, kann sie in der Regel nicht mehr gestoppt werden. Gerade bei größeren Beträgen unbedingt das übliche Procedere (Zeichnungsbefugnis, Vollmachten, 4-Augen-Prinzip) einhalten.

Weitere Informationen:

Blog „Cyberkriminalität: Risiko am Arbeitsplatz“

Broschüre „Zielscheibe Unternehmen: Cyberkriminalität“

D: DoS-Angriffe

Denial-of-Service (DoS)-Angriffe richten sich gegen Webserver, um diese zu überlasten und dadurch den Zugriff auf die Website zu stören. Ziel sind alle Internetdienste, insbesondere aber Websites mit Kundenangeboten wie Online-Shopping.

Tipps:

- Als Kunde kann man das betroffene Unternehmen kontaktieren und auf die Situation hinweisen.
- Achten Sie auf Informationen in den sozialen Medien. Die betroffenen Unternehmen informieren ihre Kunden oftmals über diese Kanäle.

E: Emotet

Emotet ist eine perfide Schadsoftware, weil sie sich in vermeintlich bekannten Mail-Absendern versteckt. Dadurch werden die Opfer leicht verleitet, auf einen Anhang (insbesondere in Form eines Office-Dokuments) zu klicken. Die Schadsoftware liest die Kontakte und Nachrichten aus und verbreitet sich über diese wieder als vermeintlich echte Mail weiter.

Tipps:

- Führen Sie alle Sicherheitsupdates regelmäßig und schnellstmöglich durch. Auch die Antiviren-Software sollte stets aktuell gehalten werden.
- Bleiben Sie wachsam - auch bei Mails von bekannten Absendern - bevor Sie ein Dokument (insbesondere Office-Dokumente) öffnen.
- Ist der Rechner befallen, hilft es zumeist nur, den Rechner komplett neu zu installieren. Deshalb ist es wichtig, seine Daten regelmäßig auf einen externen Datenträger zu speichern.
- Wer von Emotet infiziert ist, sollte unbedingt seine Mail-Kontakte über den Angriff informieren. Dieser Angriff breitet

sich über das Adressbuch aus, so dass auch Ihre Mail-Kontakte Ziel eines Emotet-Angriffs werden können.

Weitere Informationen:

Bundesamt für Sicherheit in der Informationstechnik: Aktuelle Informationen zur Schadsoftware Emotet

Bundesamt für Sicherheit in der Informationstechnik: Checkliste für den Ernstfall

F: Finanzagent

Über vermeintliche Stellenanzeigen wird ein Job als "Finanz-agent" angeboten. Voraussetzung: Man soll über sein Bankkonto Zahlungen Dritter annehmen und weiterleiten. Dann winkt eine Provision. Vorsicht: Auch wer ahnungslos als Finanz-agent missbraucht wird, kann haftbar gemacht werden.

Tipps:

Die Täter werben ihre Opfer auf verschiedene Weise an: mit seriös wirkenden Stellenausschreibungen, persönlich per Mail oder in sozialen Netzwerken. Manchmal fälschen sie sogar echte Firmen-Websites.

- Seien Sie misstrauisch, wenn Ihnen unaufgefordert leicht verdientes Geld versprochen wird.
- Prüfen Sie alle Angebote kritisch, bei denen Ihr Konto zur Abwicklung von Zahlungen für Firmen oder Personen dienen soll.
- Teilweise sind die Angebote schlecht formuliert und haben Grammatik- und Rechtschreibfehler.
- Wenn Sie eine verdächtige E-Mail erhalten haben, antworten Sie nicht und klicken Sie auf keinen Link. Geben Sie Ihre Kontodaten nicht weiter.
- Wenn Sie glauben, in einen Finanzagenten-Betrug verwickelt zu sein, stellen Sie sofort die Geldüberweisungen ein. Benachrichtigen Sie Ihre Bank und die Polizei.
- Überprüfen Sie regelmäßig Ihr Konto. Auch unerwartete Gutschriften sollten Sie stutzig machen.

Weitere Informationen:

Faltblatt „Dubioses Stellenangebot: Finanzagent“

G: Gerootet (Rooting)

Bei einem gerooteten Smartphone oder Tablet wurden die Nutzungsbeschränkungen des Betriebssystems unautorisiert entfernt. Bei Apple-Geräten spricht man auch von Jailbreaking, bei Android-Geräten von Rooting. Hat ein Angreifer Zugriff auf ein gerootetes Gerät, kann er die Sicherheitssoftware und

Sicherheitseinstellungen deaktivieren oder Schadsoftware installieren.

Tipp:

Nur Apps aus autorisierten Apps-Stores für Bankgeschäfte verwenden.

Weitere Informationen:

Broschüre „Online- und Mobile Banking: sicher über Browser und App“

I: Identitätsdiebstahl (ID-Theft)

Bei einem Identitätsdiebstahl stehlen Kriminelle persönliche Daten wie Namen, Geburtsdatum, Telefonnummer, Adresse aber auch Zugangsdaten für E-Mail- oder Social-Media-Accounts - und nutzen sie missbräuchlich beispielsweise fürs Online-Shopping mit dem gestohlenen Namen.

Tipps:

- Gehen Sie vorsichtig mit Ihren persönlichen Daten um. Es gilt das Prinzip der Datensparsamkeit! Hinterlassen Sie nur so viele Informationen, wie es notwendig ist.
- Ein Schutz kann es auch sein, verschiedene Mail-Accounts für verschiedene Zwecke anzulegen.
- Checken Sie regelmäßig alle wichtigen Accounts und Kontoauszüge.

Weitere Informationen:

Bundesamt für Sicherheit in der Informationstechnik: Identitätsdiebstahl

Bundesamt für Sicherheit in der Informationstechnik: Schutzmaßnahmen

J: Jailbreak

Bei einem Jailbreak werden Nutzungsbeschränkungen bei Apple-Geräten entfernt, ohne dass der Nutzer dazu autorisiert ist. Bei Android-Geräten spricht man von Rooting. Nach einem Jailbreak kann das Gerät zum Beispiel Apps aus nicht autorisierten Quellen installieren. Dadurch besteht eine erhöhte Gefahr, schadhafte Software herunterzuladen.

Tipp:

- Verwenden Sie für Bankgeschäfte nur Apps aus autorisierten Apps-Stores.

Weitere Informationen:

Broschüre „Online- und Mobile Banking: sicher über Browser und App“

K: Keylogger

Keylogger steht für Tastenprotokoll und bezeichnet eine Hardware oder Software, die alle Eingaben über die Tastatur ausliest. Auf diese Weise kommen Cyberkriminelle an Passwörter und Zugangsdaten.

Tipps:

- Auch die Hardware-Varianten (beispielsweise über einen Zusatzstecker) sind teilweise so geschickt versteckt, dass der Nutzer dies nicht bemerkt. Deshalb grundsätzlich keine öffentlichen PC für sensible Daten nutzen. Schützen Sie Ihren PC mit einem Passwort, wenn auch fremde Personen - zum Beispiel in von mehreren Personen benutzen Räumlichkeiten - Zugang haben.
- Vor Keyloggern schützen die üblichen Sicherheitsvorkehrungen wie Virenscanner und Firewall.

M: Malware

Malware sind schadhafte Programme auf dem PC oder mobilen Geräten (siehe auch Emotet, Trojaner, Ransomware). Meistens installiert man sie, wenn man unbekannte Anhänge öffnet oder Software von manipulierten Internetseiten runterlädt. Damit die Schadsoftware nicht erkannt wird, schaltet sie manchmal die persönliche Firewall oder das Antivirenprogramm aus. Wenn das funktioniert, kann der Angreifer die Kontrolle über alle Funktionen und Dateien der infizierten Geräte erlangen.

Tipps:

- Stellen Sie sicher, dass Ihr Antivirenprogramm mindestens einmal wöchentlich einen kompletten Suchlauf über alle Apps, Ordner und Dateien durchführt.
- Aktualisierungen der Antivirenprogramme, der Firewall, des Betriebssystems und des Internetbrowser umgehend installieren.
- Aktualisieren Sie auch sonstige Programme und Apps, sobald Updates verfügbar sind.

Weitere Informationen:

Broschüre „Online- und Mobile Banking: sicher über Browser und App“

P: Phishing

Das Wort setzt sich aus den englischen Begriffen Password und Fishing zusammen, auf Deutsch: "nach Passwörtern angeln". Beim Phishing wird zum Beispiel mittels gefälschter E-Mails oder Webseiten versucht, Zugangsdaten zu erlangen. Es kann passieren, dass Opfer unwissentlich selbst ihre Zugangsdaten in unberechtigte Hände geben. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die per E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben.

Tipps:

- Auf dem PC einen Virenscanner und eine Firewall installieren und regelmäßig aktualisieren. Auch die Software sollte immer auf dem neuesten Stand sein. Sobald Sie ein Update angeboten bekommen, nutzen Sie es und zögern die Installation nicht hinaus. Dies gilt auch für Tablets und Smartphones.
- Niemals auf Links oder Anhänge von unbekannten Absendern klicken. Absender und Mail genau prüfen. Sich nicht vom Inhalt der Nachricht unter Druck setzen lassen. Ruhe bewahren.
- Keine persönlichen Daten (PINs, Passwörter) – auch nicht verschlüsselt – auf dem PC, Tablet oder Smartphone speichern.
- Die Online-Banking-Zugangsdaten nur eingeben, wenn man sich auf der geschützten Seite der Bank befindet und eine verschlüsselte Verbindung besteht. Das lässt sich unter anderem daran erkennen, dass die Internetadresse der Bank mit https:// beginnt oder ein Schlüsselsymbol in der Browserleiste angezeigt wird.

Weitere Informationen:

Flyer „Wie schütze ich mich vor Phishing?“

Blog „Tipps zum Schutz vor Phishing im Netz“

R: Ransomware

Ransomware sind Schadprogramme, die Daten und Systeme verschlüsseln, so dass man nicht mehr darauf zugreifen kann. Diese werden dann nur gegen Zahlung eines Lösegeldes (Englisch "ransom") wieder freigegeben. Es handelt sich dabei um eine digitale Erpressung.

Tipps:

- Führen Sie alle Sicherheitsupdates der Betriebssysteme und Anwendungsprogramme schnellstmöglich durch. Halten Sie auch die Antivirensoftware stets aktuell.

- Prüfen Sie den Absender, bevor Sie auf einen Link klicken oder einen Dateianhang öffnen.
- Ist der Rechner befallen, hilft es zumeist nur, den Rechner komplett neu zu installieren. Deshalb ist es wichtig auch als privater Nutzer, seine Daten regelmäßig auf einen externen Datenträger zu speichern.
- Ziehen Sie einen Experten hinzu, und melden Sie den Fall bei der Polizei bzw. erstatten Sie Anzeige.

S: Smishing

Beim Smishing, geht es um Phishing per SMS. Der Empfänger der Textnachricht wird aufgefordert, einem Link zu folgen oder eine Telefonnummer anzurufen, um das eigene Konto zu „prüfen", zu „aktualisieren" oder zu „reaktivieren". Der Link führt das potenzielle Opfer dann zu einer gefälschten Webseite bzw. der Anruf führt zu einem Kriminellen, der sich als Mitarbeiter des echten Unternehmens ausgibt.

Tipps:

- Generell gilt: Klicken Sie nicht vorschnell auf Links oder rufen Sie nicht vorschnell die angegebene Nummer an. Nehmen Sie sich Zeit und lassen Sie sich nicht unter Druck setzen.
- Prüfen Sie den Absender bevor Sie auf Links klicken oder Anhänge und Bilddateien öffnen. Das gilt auch für Textnachrichten (SMS).
- Banken fragen niemals per Textnachricht (und auch nicht per Telefon oder E-Mail) nach Onlinebanking-Passwörtern, PINs der Kredit- oder Debitkarte oder nach anderen Sicherheitsmerkmalen und fordern auch nie dazu auf, Geld auf ein anderes Konto zu überweisen.
- Für den Fall, dass Sie den Verdacht haben, Opfer einer solchen Betrugsmasche geworden zu sein, kontaktieren Sie umgehend Ihre Bank und gegebenenfalls die Polizei.

Weitere Informationen:

Blog „Smishing, Vishing, Phishing: Achtung, Datenklau!"

T: Tech-Support-Angriffe

Vorsicht bei Anrufen vermeintlicher Bankmitarbeiter oder Software-Experten, die ihre Hilfe anbieten. Diese schlagen zum Beispiel vor, virtuellen Zugriff auf den PC zu erlauben oder sensible Daten auf einer gefälschten Bankseite einzugeben. Mittels einer schnell installierten Schadsoftware versuchen Angreifer, diese Daten auszulesen - oder den Computer zu sperren und anschließend Geld zu erpressen.

Tipps:

- Bei Zweifeln an der Seriosität des Gesprächspartners lassen Sie sich nicht überrumpeln – bitten Sie einfach um Namen

und Telefonnummer, um zurückzurufen. Überprüfen Sie vor dem Rückruf die Telefonnummer, indem Sie auf die Webseite des Unternehmens gehen, rufen Sie die Auskunft an oder schauen Sie im Telefonbuch nach.

- Achtung bei Anrufen vermeintlicher Bankmitarbeiter: Banken werden ihre Kunden nicht telefonisch kontaktieren, um eine Sicherheitsaktualisierung oder Transaktion durchzuführen. Im Zweifel auflegen und selbst bei der Bank anrufen.
- Und wenn man ganz sicher gehen will: Von einem anderen Gerät - zum Beispiel vom Handy statt vom Festnetz anrufen. Es gab schon Fälle, bei denen der Anrufer einfach in der Leitung geblieben ist.

T: Trojaner

Trojaner sind eine der ältesten und gängigsten Formen von Schadsoftware, die häufig über das Öffnen von unbekannten Dateianhängen und das unbeabsichtigte Herunterladen von Software über manipulierte Internetseiten auf den PC installiert werden (siehe auch Malware, Ransomware).

Tipps:

- Alle Sicherheitsupdates der Betriebssysteme und Anwendungsprogramme schnellstmöglich durchführen. Auch die Antiviren-Software stets aktuell halten.
- Prüfen Sie den Absender, bevor Sie auf einen Link klicken oder einen Dateianhang öffnen.
- Ist der Rechner befallen, hilft es zumeist nur, den Rechner komplett neu zu installieren. Deshalb ist es wichtig, die eigenen Daten regelmäßig auch auf einen externen Datenträger zu speichern.
- Haben Sie den Verdacht, Schadsoftware heruntergeladen zu haben, ziehen Sie einen Experten zurate und melden Sie den Fall bei der Polizei bzw. erstattet Sie Anzeige.

V: Vishing

Beim Vishing – das Wort setzt sich zusammen aus den englischen Begriffen Voice und Phishing - soll das Opfer am Telefon dazu verleitet werden, seine Daten herauszugeben oder direkt Geld an die Kriminellen zu überweisen. Kriminelle recherchieren vorab in den sozialen Medien persönliche Informationen des potenziellen Opfers und führen es damit in die Irre.

Tipps:

- Erste Regel: sich nicht unter Druck setzen lassen. Ruhig bleiben. Keine persönlichen Daten am Telefon durchgeben.
- Im Zweifel lässt man sich die Telefonnummer geben und verspricht einen Rückruf. So gewinnt man Zeit und kann die Telefonnummer der Organisation selbst nachprüfen. Natürlich darf nicht die im Display angezeigte Nummer

zurückgerufen werden, denn genau diese kann gefälscht sein.

- Bankmitarbeiter fragen niemals am Telefon nach Onlinebanking-Passwörtern, PINs der Kredit- oder Debitkarte oder nach anderen Sicherheitsmerkmalen und fordern auch nie dazu auf, Geld auf ein anderes Konto zu überweisen.
- Bei Verdacht, Opfer einer solchen Betrugsmasche geworden zu sein, umgehend die eigene Bank kontaktieren, um einen Schaden weitgehend abzuwenden.

Weitere Informationen:

Blog „Smishing, Vishing, Phishing: Achtung, Datenklau!“