2. Gefahren durch Kriminelle im Internet – gefälschte E-Mails und Websites

Webinar des Landes Niederösterreich
in Kooperation mit der Fachhochschule St. Pölten

Dipl.-Ing. Lukas Daniel Klausner, BSc

Was Sie heute erwartet

- Einführung
  - Begriffe und Konzepte, allgemeine Gefahren
- Phishing und verwandte Taktiken
  - Was ist das? Wie erkennt man es?
- CFO Fraud als konkretes Beispiel
- Gefahren durch Bank- und Kryptotrojaner

Einführung

/computer science & security /fh/// st.pölten

- »Social Engineering« oder »Social Hacking«
  - soziale Manipulation, um an Informationen zu gelangen oder Zugang zu technischen Systemen zu erhalten
- viele verschiedene Angriffspunkte
  - die meisten allerdings im Homeoffice nicht relevant, z. B.:
    - Baiting (Einschleusen von Datenträgern)
    - Dumpster Diving (Durchsuchen von Abfall, um sensible Daten zu bekommen)
    - Tailgating (Zugang zum Gebäude erschleichen)

Einführung

/computer science & security /fh/// st.pölten

- konzentrieren uns hier auf im Homeoffice mögliche Angriffe:
  - Phishing und Ähnliches
  - CFO Fraud
  - Bank- und Kryptotrojaner
- eine wichtige Regel: Trennung von Privatem und Beruflichem, wo immer möglich
  - wenn eigener Firmenlaptop: strikt trennen, was man auf welchem Computer macht
  - wenn nur ein Computer für Privates und Berufliches: separate Benutzerkonten
- nicht mit dem Firmenlaptop/-account Privates erledigen
  - (am Rande: Trennung auch aus DSGVO-Gründen wichtig)
  - insbesondere nicht auf »zwielichtigen« Websites surfen

Phishing

/computer science & security /fh/// st.pölten

- Phishing = Fishing = »Angeln«
  - mit gefälschten E-Mails, Kurznachrichten, … dazu bringen, Zugangsdaten, Passwörter, andere sensible Informationen zu verraten
- oft ungerichtet und breit gestreut
- Spear-Phishing: gezieltes Phishing auf einen kleineren Personenkreis mit größerem Aufwand für größeren Nutzen
- Vishing (= Voice Phishing): Phishing übers Telefon (vorgeblich von Ihrer Bank, einer Kreditkartenfirma, Microsoft, …)
  - Achtung: auch die Rufnummernkennung kann (ähnlich wie Absendeadresse bei E-Mails) gefälscht werden!

Wie erkennt man Phishing?

- seltsam aussehender Absendeadresse (z. B.: passt nicht zum Nachrichteninhalt)
  - aber: auch fälschbar! (E-Mails generell keine sichere Kommunikationsart)
  - bei bekannten Personen: untypische Wortwahl, Ausdrucksweise
- nicht an Sie persönlich adressiert oder seltsame Anrede
- oft (absichtlich) schlechte Rechtschreibung und Grammatik
- Betonung von Dringlichkeit, abzuwendender Gefahr, …

Wie erkennt man Phishing?

- Aufforderung zu untypischen Handlungen (Eingeben von Zugangsdaten/Passwörtern auf unbekannten, evtl. verdächtig aussehenden Websites)
  - aber: auch täuschend echt aussehende Websites möglich!
- möglicherweise gefährliche Anhänge (ausführbare Dateien wie .exe oder .bat, Microsoft-Office-Dateien mit ausführbaren Makros wie .docx, .xls, .ppt)
- im Extremfall ist Phishing selbst von bekannten Kontakten in Messengern möglich
- Vishing: z. B. Anrufe von Unbekannten, die sich als Vertreter*in von Microsoft oder anderen bekannten Firmen ausgeben

Was kann man tun?

- generell: misstrauisch sein!
- nicht auf Links in auch nur irgendwie verdächtigen E-Mails klicken
- E-Mail-Anhänge oder per Messenger verschickte Dateien im Zweifel nicht öffnen
- im Zweifel: nach Textteilen des E-Mails suchen
  - ⇒ es gibt im Internet Warnungen vor aktuell kursierenden Phishing-Mails (z. B. auf heise.de, mimikama.at, …)
- im Zweifel: rückfragen!
  - idealerweise auf anderem Kanal, z. B.: wenn verdächtiges E-Mail angeblich von einer Kolleg*in kommt, anrufen und nachfragen
- im Zweifel Websites selbst direkt ansurfen, statt Links zu folgen

Wie funktioniert Phishing psychologisch?

- Ausnutzung von Gutgläubigkeit und Vertrautheit
- Appell an die Hilfsbereitschaft
  - bzw. allgemeiner: Ausnutzung von emotional berührenden Themen, derzeit etwa viele Betrugsversuche mit Bezug zur COVID-19-Pandemie
- Missbrauch von Autoritätsvertrauen
  - z. B. E-Mails, die vorgeblich von der Bank, Kreditkartenfirma, von Vorgesetzten kommen

CFO Fraud: Einführung

- CFO = Chief Financial Officer
  - entspricht ungefähr kaufmännischer Geschäftsführung oder Finanzvorstand, also jemand mit weitreichender Entscheidungsbefugnis in Finanzangelegenheiten
- Fraud = Betrug
- CFO Fraud: Betrugsform, bei der sich Kriminelle gezielt als wichtige Personen aus der Managementebene oder aus dem Finanzbereich eines Unternehmens ausgeben (tw. in Kombination mit vorherigem Spear-Phishing auf diese Personen)
  - in den letzten Jahren häufige gewordene Form der Internetkriminalität

CFO Fraud: Vorgangsweise

/computer science & security /fh/// st.pölten

- vorgeblich vom CFO oder ähnlich wichtigen Personen stammende E-Mails oder Nachrichten, die dringlich die Überweisung großer Geldbeträge oder die Weitergabe von sensiblen Daten anfordern
- oft in Kombination mit …
  - Hinweis auf Notlage (»sitze in X fest und die Kreditkarte ist gesperrt«)
  - emotionalem Appell (»bin im Urlaub, machen Sie das bitte schnell für mich«)
  - Androhung von Konsequenzen (»kümmern Sie sich sofort darum, sonst sind Sie ihren Job los«)
  - Ausnutzung von Unsicherheit/Unklarheit (z. B. bestehende Kunden im entfernten Ausland mit angeblich neuen Kontodaten)
- … oder ähnlichen Appellen, um schnelle Reaktion zu erzwingen

CFO Fraud: Spear-Phishing

/computer science & security /fh/// st.pölten

- besonders heikel: oft erlangen Kriminelle zuerst mit Spear-Phishing Zugang zu Daten des CFO, recherchieren über Wochen und Monate mögliche Schwachstellen, …
  - unter Verwendung dieser Daten und Wissens dann Nachrichten mit Handlungsaufforderung, die durchaus glaubwürdig klingen können
- oft auch unter Nutzung leicht herausfindbarer Informationen (von der Firmenwebsite, aus Medienberichten, von sozialen Medien) Bezüge zu tatsächlich richtigen Sachverhalten in diesen Nachrichten, dadurch fallweise noch schwieriger zu entdecken
  - ⇒ misstrauisch sein und nachfragen (auf anderem Kanal!) wenn irgendetwas verdächtig aussieht (insbesondere bei unerwarteten, großen Überweisungen o. Ä.)!

Trojaner

- gebräuchliche Art von Schadsoftware (Computerviren)
- schleusen sich in das System ein (wie das Trojanische Pferd aus der Ilias, daher der Name), um dann dort kriminelle Aktivitäten zu ermöglichen oder direkt auszuführen
- oft als E-Mail-Anhang oder Ähnliches (⇒ vgl. Phishing-Methoden)
- derzeit besonders verbreitet:
  - Banktrojaner
  - Kryptotrojaner (auch »Ransomware«)

Banktrojaner

- Ziel: Zugangsdaten zu Onlinebanking oder Ähnlichem bekommen
- schon im privaten Kontext gefährlich genug – umso mehr im beruflichen, wo es um deutlich größere Beträge gehen kann
- durch Zwei-Faktor-Autorisierung (SMS oder Smartphone-App) zwar erschwert, aber nach wie vor möglich:
  - es wird einem weisgemacht, man müsse »aus Sicherheitsgründen« eine neue App am Smartphone installieren
  - in Wirklichkeit nützen Kriminelle dann diese neu installierte App, um die Zwei-Faktor-Autorisierung zu umgehen (indem sie z. B. den Sicherheitscode durch diese App zu ihnen umgeleitet bekommen)

Kryptotrojaner

- auch »Ransomware« – ransom = Lösegeld
- verschlüsseln das Computersystem bzw. das Smartphone (oder übernehmen zumindest die Kontrolle darüber) und geben das System erst nach Bezahlung eines »Lösegelds« wieder frei
  - manchmal mit Androhung, das System ganz zu löschen/sperren, wenn nicht bis zum Zeitpunkt X bezahlt wird
  - Bezahlung meist mit Kryptowährungen, damit Geldfluss nicht nachverfolgbar ist

Trojaner: Was tun?

- ähnlich wie bei Phishing: misstrauisch sein!
  - insbesondere bei verdächtigen E-Mail-Anhängen, per Messenger verschickten Dateien, …
- zusätzlich: System möglichst aktuell halten, Systemupdates frühestmöglich durchführen
  - aber: auch das hilft nicht immer – sogenannte »Zero-Day-Angriffe« nutzen bislang unbekannte Sicherheitslücken, gegen die es noch gar kein Systemupdate gibt

Trojaner: Was tun?

- Antivirensoftware nutzen (und aktuell halten)
  - aber: auch das hilft nicht immer
- zusätzliche Sicherheitsmaßnahme gegen Kryptotrojaner: regelmäßige Backups aller wichtigen Dateien und Systeme
  - im schlimmsten Fall kann das System von diesem Backup wiederhergestellt werden
  - idealerweise möglichst getrennt von anderen Systemen (manche Trojaner können auch innerhalb des Netzwerks von Computer zu Computer »springen«)
    - Backups also nicht nur auf eine zweite Festplatte im selben Computer, sondern auf eine externe Festplatte, die auch tatsächlich physisch vom System getrennt ist (sonst können Kryptotrojaner auch die einfach mitverschlüsseln)

Zusammenfassung

- Berufliches und Privates bestmöglich trennen, auch technisch (unterschiedliche Computer oder zumindest unterschiedliche Accounts)
- misstrauisch sein, wenn eine Nachricht auch nur irgendwie verdächtig wirkt
- im Zweifel: auf anderem Kanal rückfragen

Ausblick

/computer science & security /fh/// st.pölten

No.	Thema	Datum
1	Einführung in sicheres Homeoffice	15.4.2020
2	Gefahren durch Kriminelle im Internet – gefälschte E-Mails und Websites	17.4.2020
3	**Hardware- und Softwareanforderungen an sicheres Homeoffice**	**22.4.2020**
4	Sicherer Fernzugang zur IT des Unternehmens	24.4.2020
5	Sichere Chats und Kommunikationsdienste	28.4.2020
6	Sichere Audio- und Video-Konferenzen	30.4.2020
7	Soziale Interaktion und informelle Kommunikation im Homeoffice	6.5.2020
8	Sicheres gemeinsames Arbeiten an Dokumenten	8.5.2020
9	Sichere Einbindung von Smartphones/Tablets ins Homeoffice	13.5.2020
10	Cloud-Dienste oder selbst betriebene Programme	15.5.2020
11	Datenschutz und Datensicherheit im Homeoffice	20.5.2020
12	Sichere Einbindung von externen Partnern	27.5.2020