PHISHING AUF MOBILGERÄTEN

Phishing auf Mobilgeräten ist nicht nur anders, sondern auch problematischer als herkömmliche Phishing-Attacken.

Mobilgeräte werden aufgrund ihrer geringeren Phishing-Schutzeinrichtungen gern von Cyberkriminellen für Angriffe verwendet. Dabei sind die sensiblen und persönlichen Daten auf den Geräten großen Risiken ausgesetzt. Auf Mobilgeräten ist es für den Menschen und auch für die vorhandenen Sicherheitstechnologien schwer, Phishing-Angriffe zu erkennen und zu blockieren. Denn Mobilgeräte befinden sich nicht hinter schützenden Firewalls, besitzen meist keine Endpunkt-Sicherheitslösung (Anti-Malware-Schutz) und greifen auf eine Vielzahl neuer Messaging-Plattformen zu, die auf Desktops nicht verwendet werden. Darüber hinaus bietet die Nutzerschnittstelle von Mobilgeräten nicht die nötige Detailtiefe, um Phishing-Angriffe erkennen zu können (z. B. indem man den Mauszeiger über Hyperlinks bewegt, um die Ziel-URL anzuzeigen). Demzufolge fallen Mobilgerätenutzer laut IBM[1] dreimal eher auf Phishing-Betrug herein. Auch die Unmengen von persönlichen und Unternehmensdaten auf Mobilgeräten machen Smartphones und Co. zum neuen Lieblingsziel von Phishern. Leider jedoch ist seit 2011 die Zahl der Anwender, die Phishing-URLs auf ihren Mobilgeräten erhalten und antippen, jährlich um durchschnittlich 85 % gestiegen. Phishing auf Mobilgeräten ist wesentlich vielschichtiger als viele Unternehmen glauben. Um einen umfassenden Schutz vor Phishing-Angriffen zu erzielen, der auch Mobilgeräte abdeckt, müssen Sicherheits- und IT-Verantwortliche wissen, welche häufigen Irrtümer zum Thema Phishing den Blick trüben, und sich mit den Fakten vertraut machen. Nur so können sie fundierte Entscheidungen zum Schutz von Unternehmensdaten treffen.[2]

[1] https://securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/

[2] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

INHALTSVERZEICHNIS

Phishing auf Mobilgeräten – Irrtum Nr. 1

Viele glauben, dass konventionelle Phishing-Schutzmechanismen auch Mobilgeräte abdecken.

Phishing auf Mobilgeräten – Irrtum Nr. 2

Viele glauben, dass sich Phishing-Angriffe nur auf E-Mails richten.

Phishing auf Mobilgeräten – Fakt Nr. 1

Auf Mobilgeräten ist es einfacher, Nutzer in die Phishing-Falle zu locken als auf Desktop-PCs.

Phishing auf Mobilgeräten – Fakt Nr. 2

Entwicklern von Malware für Mobilgeräte, vor allem mAPT- Programmierern, gelingt es, ihre Phishing-Methoden erfolgreich in der Praxis anzuwenden.

Phishing auf Mobilgeräten – Fakt Nr. 3

Unternehmen müssen sich auch darüber Gedanken machen, dass Apps (nicht nur Menschen) unbeabsichtigt Phishing-URLs öffnen und sie nichts ahnenden Mobilgerätenutzern zur Verfügung stellen.[3]

[3] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Phishing auf Mobilgeräten – Irrtum Nr. 1

Konventioneller Phishing-Schutz eignet sich auch für Mobilgeräte.

Phishing-Mails können durch Firewalls, sichere E-Mail-Gateways, Virenschutz auf Endgeräten und durch die Aufklärung der Nutzenden zum großen Teil verhindert werden. Dieser Ansatz funktioniert relativ gut auf stationären und traditionellen Firmenrechnern, die ein Unternehmen selbst verwaltet. Auf Mobilgeräten lässt sich das nicht so einfach realisieren. Viele Mobilgeräte werden auch für persönliche Zwecke verwendet, selbst wenn es sich um Firmengeräte handelt. Phisher benutzen als das Angriffswerkzeug E-Mails, von denen laut „U.S. Consumer Device Preference Report“ von MovableInk[4] 66 % zuerst auf Mobilgeräten geöffnet werden. Zwar haben die meisten Unternehmen einen Schutz für ihre geschäftlichen E-Mails eingerichtet, jedoch eröffnen private E-Mail-Konten ein neues Einfallstor für Bedrohungen. Es gibt auch bei privaten E-Mail-Anbietenden einen standardmäßigen Phishing-Schutz, aber Angreifende finden immer neue Wege, diese Technologien zu umgehen und Mitarbeitende dazu zu verleiten, sensible Daten preiszugeben oder präparierte Apps herunterzuladen. Damit ist der Zugriff Unternehmensdaten möglich. Versierte Angreifende nutzen gezielt private E-Mail-Konten, wenn sie Firmendaten ausspähen wollen, weil sie wissen, dass für diese nicht dieselben strengen Schutzmechanismen gelten wie für Geschäfts-E- Mails. Und sie wissen auch, dass beide E-Mail-Konten auf Mobilgeräten genutzt werden. Angesichts der professionellen Optik von Phishing-Seiten (oder präparierten Webseiten, die Nutzer zur Preisgabe ihrer Daten verleiten sollen) verwundert es kaum, dass dies eine so beliebte Angriffsmethode ist. Ein kurzer Blick auf die folgenden Anmeldebildschirme verdeutlicht das Problem. Selbst erfahrenen Personen fällt es schwer, den Unterschied zwischen echten und gefälschten Nutzerschnittstellen zu erkennen, vor allem auf den relativ kleinen Mobilgeräte-Displays. Dennoch stellen E-Mails nur einen der Angriffsvektoren dar, die für Phishing genutzt werden, und Mobilgeräte eröffnen dabei völlig neue Zugangswege.[5]

Wenn die Adresszeile verborgen ist, um die URL zu verschleiern, sehen sich diese beiden Anmeldebildschirme auf Mobilgeräten zum Verwechseln ähnlich.

Abbildung 1: Darstellung einer echten und einer gefälschten Webseite; Quelle: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

[4] https://martech.org/majority-emails-opened-apple-devices-android-users-pay-attention/

[5] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Die Phishing-Kill-Chain für Mobilgeräte

Ein Fingertipp genügt, um ein Mobilgerät zu infizieren z. B. über eine präparierte URL, die im Browser-Fenster verkürzt angezeigt wird oder über eine URL, die eine App im Hintergrund ausführt und damit unbeabsichtigt eine Verbindung zu einem schädlichen Anzeigennetzwerk herstellt oder über einen Link in einer privaten E-Mail, der dazu verleitet, Firmenzugangsdaten preiszugeben. So gelangen Angreifende in die IT-Infrastruktur eines Unternehmens und können sich systematisch zu den schützenswerten Daten vorarbeiten.[6]

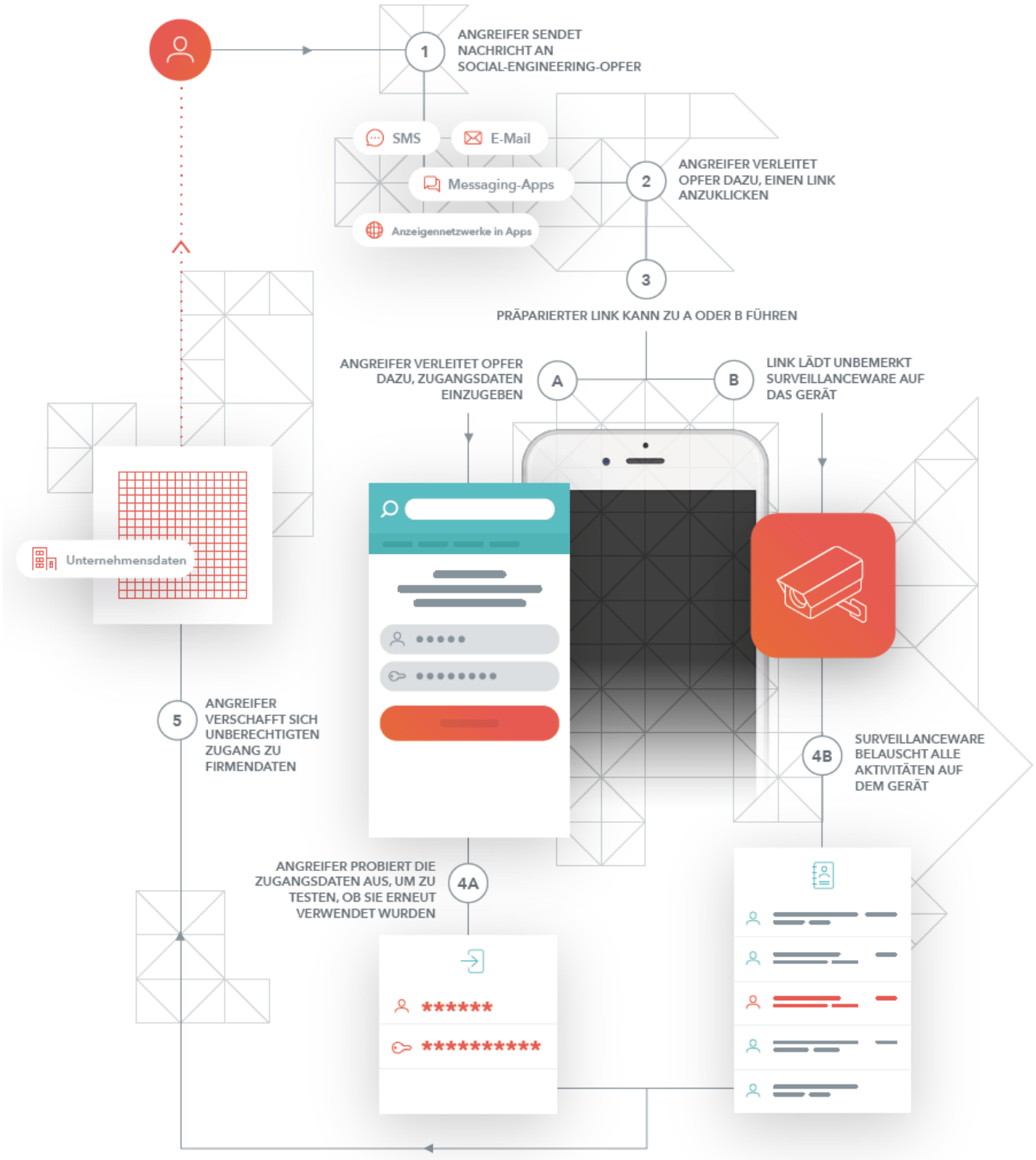

Abbildung 2: Ablauf eines Phishing-Angriffs; Quelle: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

[6] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Phishing auf Mobilgeräten – Irrtum Nr. 2

Phishing erfolgt nur über E-Mails.

Phishing-Versuche beschränken sich nicht nur auf E-Mails, denn Mobilgeräte eröffnen Angreifenden neue Angriffswege. Dabei bedienen sie sich auch SMS und MMS für Phishing sowie auch der weit verbreiteten Social-Media-Apps und Messaging-Plattformen wie WhatsApp, Facebook Messenger und Instagram. Laut einer Studie von Lookout tippten mehr als 25 % der Mitarbeitenden auf einen Link in einer SMS von einer Telefonnummer, die wie eine Nummer aus ihrer Region wirkte. Die Beispiele zeigen, dass Phisher sich längst nicht mehr auf E-Mails beschränken, sondern auch gezielt Mobilgeräte angreifen. Doch wie konnten Mobilgeräte so schnell zu einem primären Angriffsvektor für Phishing werden?

- Mobilgeräte bieten neue Messaging-Plattformen.
- Da viele dieser Geräte nicht von Sicherheitsexperten verwaltet werden und meist auch über keinen Virenschutz verfügen, sind sie Angriffen oft schutzlos ausgesetzt.
- Aufgrund der besonderen Funktionen von Mobilgeräten (wie Ortungsdiensten, Front- und Rückkameras, Mikrofon, Sprachanrufe, SMS, E-Mail und Apps) und der Tatsache, dass die Opfer ihr Telefon meist bei sich tragen, lassen sie sich effektiver überwachen.[7]

ViperRAT

ViperRAT ist eine ausgefeilte Surveillanceware (Überwachungssoftware). Die Angreifenden hinter ViperRAT locken ihre Opfer in eine Falle, indem sie sich in sozialen Netzwerken als Frauen ausgeben und die nichts ahnenden Nutzenden zum Download einer präparierten Anwendung verleiten. Nachdem sie eine persönliche Beziehung zur Zielperson aufgebaut haben, senden sie ihrem Opfer eine Nachricht über das soziale Netzwerk, in der sie es bitten, eine App herunterzuladen, um die „Kommunikation zu vereinfachen“. Angreifende können anhand der von ViperRAT gestohlenen Informationen feststellen, wo sich die Zielperson aufhält, zu wem sie Kontakt hat (einschließlich der Profilfotos der Kontaktpersonen) und welche Nachrichten sie verschickt. Außerdem haben sie Zugriff auf den Browserverlauf, Screenshots mit Daten aus anderen auf dem Gerät installierten Apps und sie können in der Nähe des Geräts geführte Gespräche und wiedergegebene Audiodaten abhören und alles sehen, worauf die Gerätekamera gerichtet wird.

Phishing-Kampagne auf Facebook

Die Experten von F-Secure entdeckten eine Phishing- Kampagne, die auf iOS und Android-Nutzende abzielt. Dabei schickten die Angreifenden der Zielperson eine Nachricht über Facebook Messenger, in der sie dem Opfer glauben machen wollten, es sei in einem YouTube-Video zu sehen. Wenn das Opfer über ein iOS- oder Android-Gerät einen Link antippte, wurde der Gerätetyp erkannt und eine entsprechende Seite angezeigt, die wie der jeweilige Facebook-Anmeldebildschirm aussah, um die Zugangsdaten des Opfers abzugreifen. Bei PC-Nutzenden sah die Nutzerschnittstelle anders aus. Diese Art von Angriff könnte Opfer mittels Social Engineering dazu bewegen, ihre Zugangsdaten für beliebige Dienste, darunter auch geschäftlich genutzte, preiszugeben.(7)

[7] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Phishing auf Mobilgeräten – Fakt Nr. 1

Auf Mobilgeräten ist es einfacher, Nutzende in die Phishing-Falle zu locken als auf Desktop-PCs.

1. Beispiel:

Studien zeigen, dass Nutzende auf einem Smartphone dreimal eher einem Link folgen würden als an einem PC. Im Vergleich zu Desktop- Computern, wo die Nutzenden den Mauszeiger über Hyperlinks bewegen können, um den vollständigen Linktext zu sehen, lässt sich die Echtheit von Links auf Mobilgeräten vor dem Anklicken wesentlich schwieriger überprüfen. Hinzu kommt die Tatsache, dass Webansichten in Apps (wie der von Facebook) es nahezu unmöglich machen, zu erkennen, welche URLs die Nutzenden gerade aufrufen. Daran wird deutlich, warum Angreifende sich verstärkt auf Mobilgeräte konzentrieren.[8]

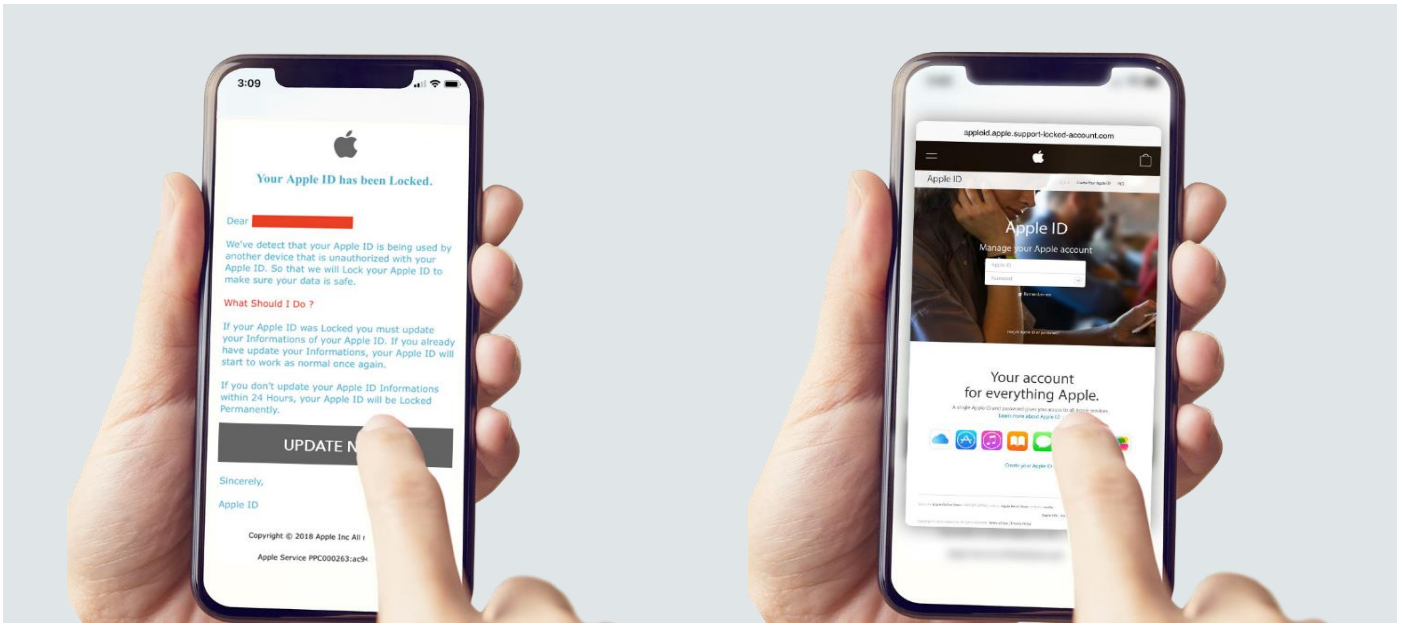

Abbildung 3: Darstellung der Schwierigkeit der Erkennung einer Weiterleitung auf eine Phishing-Seite; Quelle: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Was passiert hier? Auf einem Mobilgerät ist es wesentlicher schwerer zu erkennen, wohin ein Link führt. Hält der Nutzer einen Link in iOS gedrückt (anstatt ihn anzutippen), wird 3D Touch aktiviert und die verlinkte Seite geladen. Wenn Angreifende eine überzeugend echt wirkende Phishing-Seite bereitstellen, hätten Nutzende noch immer Schwierigkeiten, die Fälschung vom Original zu unterscheiden.[9]

8 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

9 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

2. Beispiel:

Bei einem Desktop-Monitor würde wahrscheinlich auffallen, dass eine URL „wellknownfinancial.com fakesite.xyz“ lautet anstatt „wellknownfinancial.com“, da aber mobile Browser die URL in der Adresszeile verkürzen, sieht man jeweils nur „wellknownfinancial.com“. Bisweilen ersetzt der Browser die URL sogar durch den Namen des Unternehmens, auf dessen Website zugegriffen wird (siehe Abbildung unten). So lässt sich deutlich schwerer erkennen, ob eine URL echt ist. Mobile Browser verbergen auch oft die Website-URLs in der Adressleiste, während die Anwendenden auf dem Bildschirm scrollen, und limitieren die in der Adressleiste angezeigten Zeichen in Abhängigkeit von der Bildschirmbreite. Solche an sich durchaus nützlichen Designoptimierungen erleichtern es Angreifenden, ihre Phishing-Attacken auszuüben.[10]

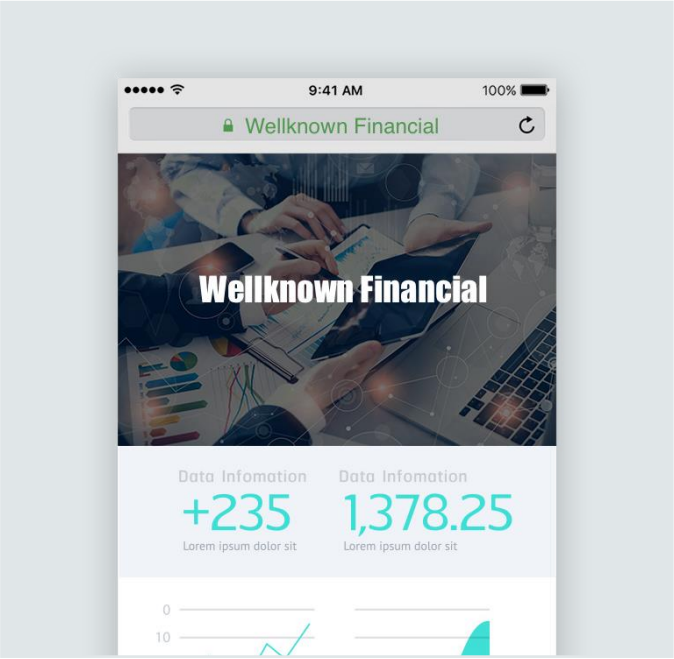

Abbildung 4: Darstellung der Schwierigkeit der URL-Überprüfung auf Mobilgeräten; Quelle: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Was passiert hier? In der Adresszeile wird nur der Firmenname angezeigt, nicht aber die URL.

3. Beispiel:

Wenn ein Mobilgerät durch eine Firewall geschützt ist und Nutzende einen Phishing-Link anklicken, greift die Firewall des Unternehmens ein und stoppt die Verbindung nach außen. Da man sich mit einem Mobilgerät aber die meiste Zeit außerhalb des Schutzbereichs bewegt, kann die Firewall einen Mitarbeitenden (z. B. auf seinem Heimweg im Zug) nicht davor bewahren, eine präparierte URL aufzurufen. Somit haben Angreifende leichtes Spiel und können ungehindert in das Netzwerk des Unternehmens eindringen – sofern das Unternehmen seinen Schutz nicht auch auf Mobilgeräte ausgedehnt hat.[11]

10 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

11 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Phishing auf Mobilgeräten – Fakt Nr. 2

Entwickelnden von Malware für Mobilgeräte, vor allem mAPT-Programmierenden, gelingt es, ihre Phishing-Methoden erfolgreich in der Praxis anzuwenden.

Phishing auf Mobilgeräten ist in zunehmendem Maße das erste Angriffswerkzeug bei großangelegten, komplexen Angriffen. Zu den häufigsten Bedrohungen zählen Mobile Advanced Persistent Threats (mAPT). Der Ausdruck „Advanced Persistent Threat“ bezeichnet den zielgerichteten, anhaltenden, effektiven Angriff einer Gruppe (in der Regel ein Nationalstaat) auf die Behörden anderer Nationalstaaten, Groß- und Mittelstandsunternehmen oder Einzelpersonen, um über einen längeren Zeitraum Informationen auszuspähen, die dem persönlichen finanziellen Gewinn der Angreifenden oder der Spionage dienen. Mit mAPT wird diese Form der Bedrohung nun auch auf Mobilgeräte ausgeweitet. Die nachfolgende Abbildung zeigt ein paar Beispiele aus der Praxis. Da mAPT-Angriffe eine neue Ebene komplexer Bedrohungen darstellen, ist hier besondere Wachsamkeit geboten.[12]

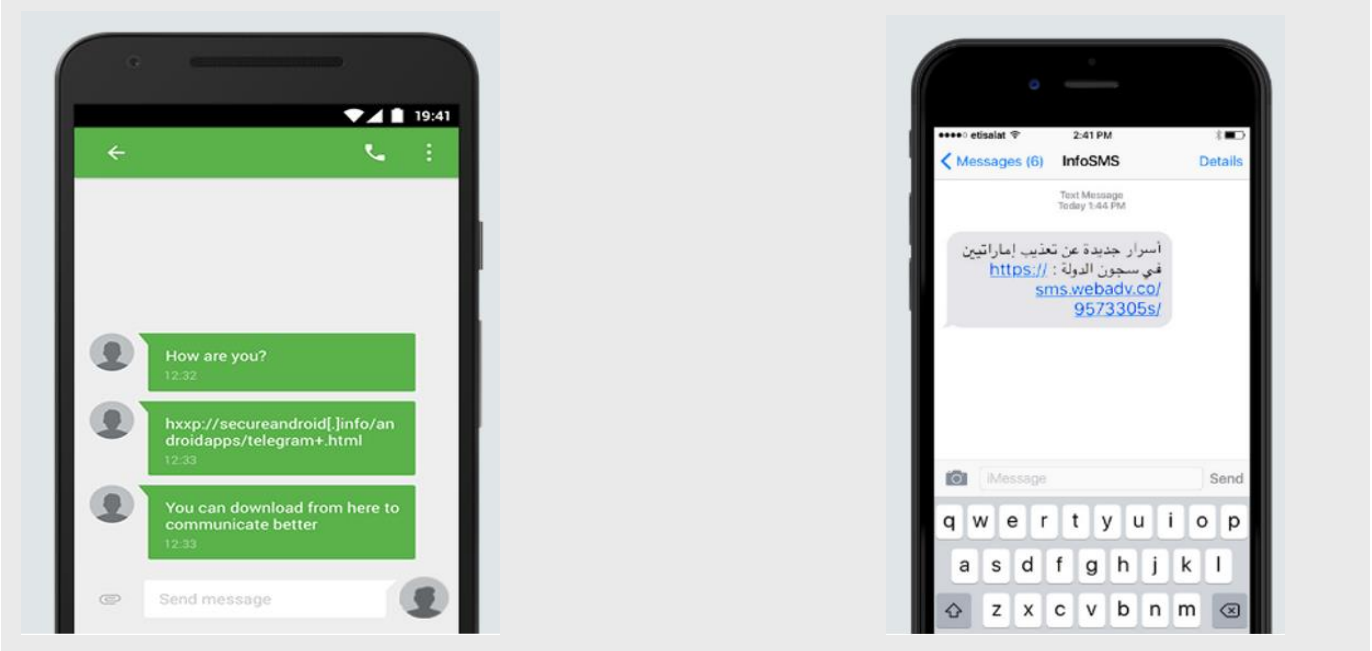

Abbildung 5: Darstellung einer SMS von Dark Caracal (links) und einer Phishing-SMS von Pegasus (rechts); Quelle: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

- **Dark Caracal**

  Dark Caracal versendet Phishing-Nachrichten über WhatsApp und Facebook, um potenzielle Opfer dazu zu verleiten, Android-Malware über präparierte Links herunterzuladen. Die Android-Malware namens Pallas überwacht dann das Gerät des Opfers und sammelt große Mengen an Daten. Dark Caracal richtet sich vor allem an Regierungsbehörden, das Militär, Versorgungsunternehmen, Finanzinstitutionen sowie Unternehmen aus der Fertigungs- und Verteidigungsindustrie. Die dabei ausgespähten Daten sind sehr umfangreich, darunter Dokumente, Anrufprotokolle, Audioaufnahmen, abgesicherte Inhalte von Messaging-Clients, Kontaktdaten, SMS/Textnachrichten, Fotos und Kontoinformationen.[13]

- **Pegasus**

  Die Surveillanceware (Überwachungssoftware) Pegasus erlangte weltweite Aufmerksamkeit durch die besonders schwerwiegenden Folgen, die solche Angriffe nach sich ziehen. Dabei senden die Pegasus-Hacker ihren Opfern eine Phishing-Nachricht per SMS. Wenn das Opfer sie anklickt, wird eine Kette von Ereignissen ausgelöst, die unbemerkt im Hintergrund ablaufen. Diese auf iOS-Geräte ausgelegte Angriffsmethode ist eine der professionellsten, die je gesehen wurde. Auf dem Gerät selbst belauschte Pegasus sämtliche Aktivitäten und sammelte dabei enorme Mengen sensibler Daten.[14]

12 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf
13 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf
14 https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-WP-DE.pdf

Phishing auf Mobilgeräten – Fakt Nr. 3

Unternehmen müssen sich auch darüber Gedanken machen, dass Apps (nicht nur Menschen) unbeabsichtigt präparierte URLs öffnen und sie nichts ahnenden Mobilgerätenutzenden zur Verfügung stellen.

URLs werden aber nicht nur von Anwendenden geöffnet (bzw. angeklickt). Auch in die Codebasis von Apps sind URLs eingebettet und rufen Informationen in Echtzeit ab. Diese Funktion nutzen Angreifende aus, um wertvolle Daten von Opfern auszuspähen. Damit müssen Unternehmen nun eine weitere Angriffsfläche absichern: seriöse Apps, die auf präparierte URLs zugreifen.

App-Entwickelnde verdienen ihr Geld oft mit Werbung. Dazu integrieren sie Anzeigen-SDKs in den App-Code. Diese SDKs stellen dann im Hintergrund eine Verbindung zu URLs her, um den Nutzenden Anzeigen einzublenden. Wenn nun die Angreifer ein Anzeigen-SDK einer seriösen App steuert, kann er mithilfe des SDK auf schädliche URLs zugreifen und den Nutzenden Werbung anzeigen, die ihn dazu verleiten sollen, vertrauliche Daten preiszugeben.

Solche Bedrohungen nutzen zwar Hintergrundfunktionen aus, aber Phishing-Attacken müssen nicht zwangsläufig versteckt ablaufen, um effektiv zu sein.