turingpoint.

Phishing-Risiko bei Verwendung der eID

Version 1.1

Whitepaper

Till Oberbeckmann (turingpoint GmbH)

Dokumentinformationen

Dokumententitel	Phishing bei Verwendung der eID
Dokumentenklassifikation	Öffentlich
Dokumententitel	Whitepaper

Dokumentenversion

Version	**Autor**	**Datum**
V1.1	Till Oberbeckmann (turingpoint GmbH)	6. Dez. 2022
V1.0	Till Oberbeckmann (turingpoint GmbH)	29. Juli 2022

Inhaltsverzeichnis

Ausgangssituation

Verwaltungsdienstleistungen werden in Deutschland häufig noch durch analoge Tätigkeiten durchgeführt. Laut einer Umfrage haben im Jahre 2021 in Norwegen rund 92% der Bevölkerung mit staatlichen Behörden über das Internet interagiert. Im Vergleich dazu waren es in Deutschland nur knapp 50%[1]. Eine Betrachtung möglicher Gründe hierfür zeigt schnell, dass verschiedene Verwaltungstätigkeiten häufig veraltete oder analoge Prozesse beinhalten.

Weiterhin sind zur Verfügung gestellte Online-Angebote meist nicht zufriedenstellend, da beispielsweise funktionale Einschränkungen, Barrieren der Benutzerfreundlichkeit oder Schwächen in der IT-Sicherheit der Systeme vorliegen. Ein hoher personeller Aufwand, da Mitarbeitende der Verwaltung zum Beispiel gesuchte Akten manuell aus dem Archiv suchen müssen, und persönlicher Aufwand, da Bürgerinnen und Bürger den Gang zur zuständigen Behörde antreten müssen, geht damit einher. Ebenso entstehen durch Terminvereinbarungen oder Vorgänge wie Post-Ident Verfahren Wartezeiten, welche die Abwicklung der Vorgänge verzögern. Hinzu kommt die vertane Zeit durch menschliche Fehlerquellen. Fehler, wie beispielsweise Tippfehler, sind menschlich, infolgedessen ist das Risiko für Fehlerquellen in analogen Prozessen deutlich erhöht gegenüber durchdachten digitalisierten Lösungen. Nicht zu vergessen, der Papierverbrauch und Postverkehr, der durch Papieranträge und Kommunikation per Brief entsteht.

Digitalisierung ermöglicht es potenziell, Bürgerinnen und Bürgern das Leben zu erleichtern. Das ist gut und ein erstrebenswertes Ziel. Insbesondere eine Digitalisierung der Verwaltung kann eine deutliche Vereinfachung und Beschleunigung der Prozesse bewirken. Da dies jedoch ein Bereich ist, in dem eine Vielzahl von personenbezogenen und anderen sensiblen Daten verarbeitet werden, ist es unabdingbar, dass die Sicherheit dieser Daten zu jedem Zeitpunkt des Prozesses sichergestellt ist.

Die eID-Funktion des neuen deutschen Personalausweises speichert Informationen der Identität der Ausweis innehabenden Person in digitaler Form auf diesem ab und ist für alle Personen ab 16 Jahren standardmäßig aktiviert. Diese Online-Ausweisfunktion ermöglicht eine digitale Identifikation der eigenen Identität.

Der im Jahre 1994 in Japan entwickelte QR-Code (*Quick Response*) ist ein zweidimensionales maschinenlesbares optisches Etikett, welches Informationen oder Daten, wie beispielsweise Links, Klartext, Adressen, Geo-Locations oder Kontaktinformationen, enthalten kann. QR-Codes weisen eine erheblich höhere Robustheit und Informationsdichte auf als herkömmliche Strichcodes. Dies macht QR-Codes zu einem beliebten Mittel, welches in unterschiedlichen Branchen genutzt wird.[2]

---

[1] https://de.statista.com/statistik/daten/studie/73560/umfrage/ineraktion-mit-staatlichen-behoerden-ueber-das-internet-im-laendervergleich/ (abgerufen 27.07.2022)

[2] T.T. Dayaratne: *A Framework to Prevent QR Code Based Phishing Attacks*. 2016

Problemdefinition

Da es sich im Rahmen der eID-Thematik um die Verarbeitung von sensiblen Daten handelt, ist es besonders notwendig, diese vor Missbrauch zu schützen. Eine Gefahr stellt hierbei der Phishing-Angriffsvektor dar. Durch Phishing kann eine angreifende Person einen legitimen Datenfluss mit einem Service starten, die Session-Informationen der angreifenden Person an ein Opfer weiterleiten und dieses dazu bringen, sich mit der Session der angreifenden Person zu identifizieren.

Beispiel Phishing-Angriff anhand Magnus Flow

Im Speziellen für den Anwendungsfall von Digital Service und dem Magnus Flow unter der Verwendung eines QR-Codes könnte ein Phishing Angriff folgendermaßen ablaufen:

- Die angreifende Person startet einen legitimen eID-Identifizierungsflow
- Die angreifende Person liest den QR-Code von der angezeigten Seite - der QR-Code enthält *tcTokenUrl* und eine *widgetSessionId*, mit der das UseID-Backend die Instanz des Widgets identifizieren kann
- Die angreifende Person erstellt eine Phishing-Website, die wie der ursprüngliche eService aussieht und eine gefälschte Version des Widgets mit dem QR-Code der angreifenden Person enthält
- Die angreifende Person bringt das Opfer dazu, die Website zu öffnen und einen Identifikationsfluss mit dem QR-Code der angreifenden Person zu starten.
- Das Opfer scannt den QR-Code mit seinem Smartphone und öffnet den eID-Client
- Der eID-Client holt sich den *tcToken* der angreifenden Person mit der tcTokenUrl aus dem QR-Code - der tcToken enthält die *sessionID* der angreifenden Person
- Das Opfer identifiziert sich durch Scannen des Ausweises
- Die mobile App sendet die Identitätsdaten des Opfers an den eID-Server mit der sessionID der angreifenden Person
- Die mobile Anwendung sendet eine Erfolgsmeldung an das UseID-Backend mit der *widgetSessionID* der angreifenden Person
- Das UseID-Backend gibt die Erfolgsmeldung an das Widget der angreifenden Person weiter, unter Verwendung der widgetSessionID
- Das Widget leitet den Browser der angreifenden Person auf die *refreshAddress* des legitimen eService um
- Der eService holt sich die Identitätsdaten der betroffenen Person vom eID-Server unter Verwendung der sessionID der angreifenden Person

- Die angreifende Person ist nun mit der Identität der betroffenen Person auf der Website angemeldet

Beispiel Phishing-Angriff anhand der MTG Demo App

Auch bei Anwendungen ohne QR-Code ist es möglich Phishing Angriffe durchzuführen, wie man es anhand der MTG Demo App sehen kann. Dieser Angriff ist nur möglich, wenn der eService Session Informationen in der tcTokenURL aufführt, so dass die angreifende Person in der Lage ist, die refreshAddress des Opfers zu ermitteln.

Der konkrete Phishing Angriff könnte folgendermaßen ablaufen:

- Die angreifende Person startet einen legitimen eID-Identifizierungsflow
- Die angreifende Person erstellt eine Phishing-Website, die wie der ursprüngliche eService aussieht und baut die tcTokenURL ein
- Die angreifende Person bringt das Opfer dazu, die Phishing Website zu öffnen und die Identifizierung zu starten - über den modifizierten Link wird der eID-Client gestartet und das Opfer durchläuft den eID-Flow
- Parallel entnimmt die angreifende Person die refreshAdress aus dem tcToken
- Der eID-Client schickt die Daten des Opfers über den eID-Server mit der sessionID der angreifenden Person
- Bevor der eID-Client das Opfer zurück zur Anwendung über die refreshAdress leiten kann, ruft die angreifende Person die refreshAdress auf - Die angreifende Person muss die refreshAdress in sehr kurzen Intervallen aufrufen, um sicherzustellen, dass er vor dem Opfer auf die Seite zugreift
- Die angreifende Person ist nun mit der Identität des Opfers eingeloggt

Die Folgen des Angriffs können von Identitätsdiebstahl (Beantragung einer Kreditkarte/SIM-Karte), über die Offenlegung von sensiblen Daten (Adresse, Steuer-ID, etc.) bis hin zu mutwilligem Schaden an Personen (Falschangaben in Behördenformularen) reichen. Deshalb ist es wichtig von Anbieterseite, das Risiko für Nutzende, Opfer eines Phishing Angriff zu werden, so weit wie möglich zu reduzieren.

Weitere Angriffsarten

Bei den Angriffsarten wird von unserer Seite unterschieden, ob das Opfer gezielt angesprochen wird oder ob versucht wird, viele Personen gleichzeitig anzugreifen.

Massen-Phishing

Bei groß angelegten Angriffen wird versucht, mehrere Personen gleichzeitig anzugreifen. Hierfür startet eine angreifende Person zahlreiche Identifizierungs-Flows und sendet die Links bzw. QR-Codes an viele verschiedene Personen. Solange eine Person aus dieser großen Gruppe den Identifizierungs-Flow für die angreifende Person durchläuft, ist die angreifende Person mit der Identität dieser Person angemeldet und der Angriff war erfolgreich.

Da wie angesprochen bei diesem Angriff zahlreiche Verbindungen geöffnet werden, sollte dies anhand der Anzahl der Zugriffe auf den Webserver gut zu monitoren sein. Des Weiteren kann eine zeitliche Beschränkung der Token das Risiko für solche Angriffe deutlich reduzieren.

Ein weiterer Ansatz hingegen wäre, nur einen QR-Code zu erstellen und diesen an viele Personen zu senden. Da in diesem Szenario nur ein Identifizierungs-Flow gestartet wird, ist es nur sehr schwer möglich, diesen Angriff mithilfe von Monitoring zu detektieren.

Nichtsdestotrotz lässt sich das Risiko dieser Angriffsart durch einen zeitbasierten Token massiv reduzieren, da ich als angreifende Person hoffen muss, dass das Opfer in einem sehr begrenzten Zeitraum den Identifizierungs-Flow für mich durchläuft.

Fortgeschrittenes Massen-Phishing

Eine andere Angriffsart wäre ein dynamisches Vorgehen, bedeutet, dass ich als Angreifer erst den QR-Code auslesen und in meine Phishing-Seite einbette, wenn das Opfer auf meine Seite kommt. Bei dieser Angriffsart wäre eine zeitliche Beschränkung des Tokens hinfällig. Auch durch Monitoring Maßnahmen wäre es nicht möglich, solch einen Angriff zu erkennen.

Des Weiteren kann man z.B. auch eine Captcha Aufgabe umgangen werden, indem man diese einfach bis zum Opfer durchreicht und dieser das Captcha löst.

Gezieltes Phishing

Bei einem gezielten Phishing Angriff wird das Opfer gezielt angesprochen, dies kann über verschiedene Kanäle wie z.B. E-Mail, Live-Chat oder auch in Persona. Auch in diesem Fall wird versucht, das potenzielle Opfer dazu zu bringen, auf meinen Link zu klicken bzw. den von mir zur Verfügung gestellten QR-Code zu scannen.

Diese Art von Angriff zu vermeiden, ist für Anbietende nahezu unmöglich.

Minimierung des Phishing Risikos

Phishing ist eine immer wiederkehrende Bedrohung, die auf Schwächen der Menschen abzielt. Daher ist es wichtig, hinreichende Sicherheitsmechanismen zur Mitigation des Phishing-Risikos vorzunehmen.

Generische Token URL

Informationen, über die sich eine bestimmte Session bzw. Person eindeutig identifizieren lassen, sind ein begehrtes Ziel von Angreifenden und nicht zuletzt in vielen Fällen eine wichtige Voraussetzung für einen erfolgreichen Phishing-Angriff. Daher sollte darauf geachtet werden, möglichst wenig Session-Informationen über URL Parameter oder Cookies offenzulegen. Die Generierung eines tcToken sowie QR-Codes sollte daher über eine generische URL erfolgen. Wird bei jedem Aufruf dieser URL ein neuer QR-Code generiert, ist es einer angreifenden Person nicht ohne Weiteres möglich, die Adresse, des eigen generierten QR-Codes weiterzugeben. Dies erhöht die Komplexität und den Aufwand für die angreifende Person.

Time based Token

Zur Verringerung des Zeitfensters eines Phishing-Angriffes sollte die Gültigkeitsdauer des Token bzw. des QR-Codes eingeschränkt werden. Je kürzer die Gültigkeit eines Token ist, desto geringer ist die Wahrscheinlichkeit, dass ein Angriff erfolgreich ist. Ist beispielsweise ein QR-Code nur für ein Zeitfenster von drei Minuten gültig, so müsste eine angreifende Person in dieser Zeit den QR-Code in die Phishing-Website einbinden und eine Zielperson dazu bringen, diese zu besuchen, den Code zu scannen und den Identifizierungsprozess vollständig durchzuführen. Würde dieser Prozess nicht vollständig durchgeführt werden können, so müsste die angreifende Person einen neuen QR-Code generieren und den Angriff erneut starten. Bei der Implementierung von Time-based Token ist jedoch darauf zu achten, dass der Gültigkeitszeitraum so kurz wie möglich, aber auch so lange wie nötig gültig ist, um eine legitime Identifikation durchzuführen.

Zusätzliche Sensibilisierung & Metadaten

Phishing-Angriffe zielen immer auf Schwachstellen von Menschen ab. Daher ist es besonders wichtig, eine gewisse Sensibilisierung in diesem Bereich herzustellen. Unternehmen nutzten hierfür gerne die Simulation von E-Mail-Phishing Angriffen, um die Awareness ihrer Mitarbeitenden gegenüber gefälschten E-Mails zu erhöhen. Einzelpersonen

hingegen werden in den seltensten Fällen an Phishing-Simulationen teilnehmen. Um dennoch auf die Risiken von Phishing hinzuweisen, können direkt in der Anwendung Warnhinweise angezeigt werden. Beispielsweise können Benutzende in Textform gebeten werden, die URL des angestoßenen eService zu überprüfen und die nachfolgende Identifikation nur dann durchzuführen, wenn diese mit der in der App angezeigten URL übereinstimmen. Zusätzlich dazu wäre es auch möglich, Metadaten, wie die IP-Adresse, User-Agent oder Geo-Location, des Gerätes, mit dem der QR-Code erstellt wurde, in der App anzuzeigen. Dies würde der Person, welche die Identifikation durchführen möchte, die Möglichkeit geben, diese Daten mit den eigenen abzugleichen. Hierbei ist jedoch zu beachten, dass Informationen wie die IP-Adresse zu den persönlichen Daten gehören und somit besonders schützenswert sind. Daher muss hierbei darauf geachtet werden, dass die Sammlung bzw. Übertragung solcher Daten mit der DSGVO vereinbar ist.

Monitoring & IP Blocking

Zum Schutz der Webanwendung des eService, auf dem der QR-Code Nutzern initial angezeigt wird, kann ein Monitoring- und Analyseverfahren oder eine Web Application Firewall (WAF) betrieben werden. Durch die Untersuchung der Kommunikation der Anwendung sollen so Auffälligkeiten oder Anomalien erkannt, analysiert und verdächtige Aktionen unterbunden werden. Beispielsweise könnten Anfragen bestimmter Hosts, von denen eine Vielzahl von QR-Codes generiert werden, blockiert werden.

Dies könnte insbesondere in Kombination mit Time based Token wirksam sein, da eine angreifende Person potenziell regelmäßig neue QR-Codes generieren müsste, sobald die Gültigkeit abgelaufen ist und der Angriff zu diesem Zeitpunkt nicht erfolgreich durchgeführt wurde.

Vermeidung von Schnittstellen

Besonders kritisch für den Abfluss von Daten ist der Übergang von der eID-App zurück in die Webanwendung des eService. Zu diesem Zeitpunkt hat sich die Ausweis inhabende Person bereits identifiziert und diese persönlichen Daten müssen an den eService übermittelt werden. Geschieht diese Übermittlung per “Redirection” oder mittels Server-Sent Event zur ursprünglichen Browser-Session, wird der Prozess auf dem Client abgeschlossen, von der der ursprüngliche QR-Code generiert und Flow gestartet wurde. Würde hierbei eine angreifende Person A einen Flow im eigenen Browser anstoßen und anschließend eine Zielperson B dazu bringen, sich in dem durch Person A angestoßenen Flow über die eID zu identifizieren, könnte, nach erfolgreichem Abschluss, Person A die Daten von Person B im Browser der ursprünglichen Session abrufen.

Um das Phishing-Risiko an dieser Stelle zu minimieren, sollte diese Rückführung bzw. dieses Verhalten vermieden werden. Hierbei gibt es verschiedene Methoden: Eine Möglichkeit wäre es, den Abschluss des Prozesses nicht im Browser des Clients, von dem der Flow gestartet wurde, durchzuführen, sondern eine neue Session in einem neuen

Browserfenster auf dem Mobilgerät, auf dem die eID Identifikation stattgefunden hat, zu starten. Hierbei ist darauf zu achten, dass keine Informationen über die neu erstellte Session bereits in den vorangestellten Schritten offengelegt werden, sowie der *SessionIdentifier* zufällig und unabhängig von den Daten der Anwendung gewählt wird. Dadurch könnte sichergestellt werden, dass die Identifikation durch die eID und die Übermittlung der Daten an den eService auf dem gleichen Gerät erfolgen.

Alternativ könnte, nachdem die erfolgreiche Identifikation mit der eID stattgefunden hat, ein zusätzlicher Schritt eingeführt werden, bei dem die sich ausweisende Person die eigene E-Mail-Adresse angibt. An diese wird anschließend eine E-Mail versendet, welche einen Link enthält, unter dem der Prozess mit dem eService abgeschlossen werden kann. Der SessionIdentifier sollte auch in diesem Szenario zufällig und unabhängig gewählt und nicht im Vorfeld offengelegt werden.

Zusammenfassung & Sicherheitseinschätzung

Abschließend bleibt zu sagen, dass die Gefahr von Phishing immer vorhanden sein wird und man von Seiten der Anbietenden lediglich dazu beitragen kann, das Risiko für die Nutzenden zu reduzieren.

Die Verwendung eines QR-Codes bietet ein größeres Risiko, da dieser sehr einfach an andere weitergegeben werden kann und dies von Anbietenden auch nicht verhindert werden kann.

Risiko für Grundsteuer-Anwendung

Das Risiko für einen Angriff auf die Grundsteuer Anwendung wäre nach Umsetzung aller vorgeschlagenen Härtungsmaßnahmen ein vertretbares Risiko, solange die Identifizierung als letzter Schritt stattfindet.

Ein Angriff auf die Grundsteuer Anwendung ist unserer Ansicht nach jedoch eher unwahrscheinlich, da die Auswirkungen eines Angriffs sich stark in Grenzen halten. Eine angreifende Person könnte lediglich Formulardaten ändern, dies kann zwar auch die Bankverbindung betreffen, jedoch ist im Vorhinein nie bekannt, ob man eine Gutschrift oder eine Nachzahlung erhält.

Ist das Ziel einer angreifenden Person einzig und allein Schaden bei dem Phishing-Opfer anzurichten, so könnte die angreifende Person nach einem erfolgreichen Phishing-Angriff die Daten der betroffenen Person verfälschen und somit Falschangaben machen. Dies ist jedoch ein rein destruktives Motiv, von dem eine angreifende Person keinen direkten Mehrwert hat. Insofern ist fraglich, inwieweit dies ein realistisches Angriffsziel ist.

Darüber hinaus bietet die angestrebte Lösung der Grundsteuer Anwendung den Vorteil, dass die eID-Client Anwendung lediglich für Mobilgeräte von Android und iOS verfügbar

gemacht werden soll. Apps auf Mobilgeräten sind Desktopanwendungen in dem Aspekt überlegen, dass diese in geschützten Sandbox Umgebungen ausgeführt werden und infolgedessen ein höheres Sicherheitsniveau aufweisen. Daher ist die Vermeidung einer eID-Client-Desktop-Anwendung ein Vorteil in Bezug auf die Sicherheit.