EVIDEN

Schutz gegen Phishing

Technische Lösungen für die Praxis

Management Summary

Phishing-Angriffe haben sich in den letzten Jahren zu einer der häufigsten und am schnellsten wachsenden Form der Cyberkriminalität entwickelt. Beim Phishing werden IT-Benutzer dazu verleitet, vertrauliche Informationen preiszugeben, in der Regel durch irreführende E-Mails oder Nachrichten, die zu betrügerischen Webseiten führen. Mehrere medienbekannte Vorfälle, wie das Eindringen in das IT-System von SolarWinds[1] und das Hacken von Colonial Pipeline[2], haben das Ausmaß dieses Problems deutlich gemacht. Phishing hat sich zu einer Bedrohung entwickelt, deren Bekämpfung noch schwieriger geworden ist, seitdem die Angreifer künstliche Intelligenz nutzen.

Die Zahl der Phishing-Vorfälle ist in den letzten Jahren sprunghaft angestiegen: Im Jahr 2022[3] wurden über 500 Millionen Angriffe gemeldet, wobei die Zahl der Angriffe zwischen Mai und Oktober 2022 um 61 % gestiegen ist[4]. In den USA gab es im Jahr 2022 rund 300 497 Phishing-Opfer. Mehrere Gesetze in Frankreich, Deutschland und anderen Ländern schreiben implizit einen Phishing-Schutz vor, um diese Bedrohung zu bekämpfen. Sichere Passwörter, Einmal-Passwörter (OTP), biometrische Authentifizierung und CAPTCHAs erhöhen zwar die Sicherheit, verhindern aber keine Phishing-Angriffe. Die zertifikatsbasierte Authentifizierung, unterstützt durch eine Public-Key-Infrastruktur (PKI), ist eine wirksame Gegenmaßnahme gegen Phishing. Mit dieser Technologie kann die Echtheit des öffentlichen Signaturschlüssels des Kunden überprüft werden, was Phishing-Versuche erheblich erschwert.

Anstelle einer PKI und digitaler Zertifikate kann auch die Authentifizierungsinfrastruktur des Industrieverbands FIDO zur Authentifizierung des öffentlichen Signaturschlüssels des Kunden verwendet werden, der zum Schutz vor Phishing eingesetzt wird. Diese Alternative ist besonders attraktiv, wenn keine PKI verfügbar ist. Sowohl die zertifikatsbasierte als auch die FIDO-Authentifizierung werden noch sicherer, wenn Token-Binding eingesetzt wird. Der kryptografische Ende-zu-Ende-E-Mail-Schutz, einschließlich der Verwendung von Verschlüsselung und digitalen Signaturen, ist eine weitere wichtige Technologie zum Schutz vor Phishing. Sie erhöht die E-Mail-Sicherheit und erschwert es Angreifern, sich als legitime Absender auszugeben.

Eviden bietet eine Reihe leistungsfähiger Sicherheitslösungen zur Verhinderung von Phishing-Angriffen, darunter zertifikatsbasierte Authentifizierung und FIDO-Authentifizierung mit Token-Binding sowie kryptografischen E-Mail-Schutz. Die wichtigsten dieser Lösungen sind das CardOS-Betriebssystem, IDnomic PKI (einschließlich eines Cloud-basierten PKI-as-a-Service-Angebots) und cryptovision GreenShield. Interessierte Organisationen sollten Eviden kontaktieren, um ihre Anforderungen zu besprechen.

1. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
2. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
3. https://www.forbes.com/advisor/business/phishing-statistics/
4. tinyurl.com/mryn2zz9

Inhalt

Einführung

Phishing-Angriffe sollen IT-Anwender dazu zu verleiten, Anmeldedaten oder andere sensible Informationen preiszugeben. In der Regel stehen am Anfang gefälschte E-Mails oder andere Nachrichten, die den Empfänger auf eine betrügerische Webseite führen. In den letzten Jahren hat die IT-Welt einen alarmierenden Anstieg von Phishing-Angriffen erlebt, was diese Technik zu einer der dominierenden und am schnellsten wachsenden Form der Cyberkriminalität macht. In den Medien wurde über zahlreiche Beispiele von Sicherheitsverletzungen durch Phishing berichtet (siehe nebenstehende Kästen).

Die folgenreichsten Phishing-Angriffe

SolarWinds: Die im Dezember 2020 entdeckte Sicherheitslücke bei SolarWinds war die Folge eines ausgeklügelten Cyberangriffs, der verschiedene US-Behörden und private Organisationen betraf. Dabei fügten Hacker schadhaften Code in ein Software-Update für die Orion-Plattform von SolarWinds ein, ein weit verbreitetes Tool zur Netzwerküberwachung. Wenn die Kunden dieses kompromittierte Update installierten, konnten sich die Angreifer unbefugten Zugang zu ihren Netzwerken verschaffen. Der Angriff begann damit, dass ein Konto gehackt wurde. Von dort aus konnten die Angreifer Phishing-E-Mails verschicken, um die Opfer dazu zu bringen, auf einen Link zu klicken, über den ein Backdoor-Trojaner installiert wurde. Der durch die Sicherheitsverletzung bei SolarWinds entstandene finanzielle Schaden wird auf rund 90 Millionen US-Dollar geschätzt.[5]

Colonial Pipeline: Der Hacker-Angriff auf die Colonial Pipeline ereignete sich im Mai 2021 und startete eine Ransomware auf den IT-Systemen einer der größten Ölpipelines in den Vereinigten Staaten. Die Angreifer verschlüsselten die Daten der Pipeline und forderten erfolgreich ein Lösegeld im Austausch gegen den Entschlüsselungsschlüssel. Auch hier begann der Hack mit einem Phishing-Angriff.[6]

Gesundheitsbehörde in den USA: Im Februar 2022 wurden nach einem erfolgreichen Phishing-Angriff auf eine Gesundheitsbehörde im Bundesstaat Washington die medizinische Daten von mehr als 1.200 US-Bürgern offengelegt.[7]

NFT Investments: Im Januar 2023 wurde NFT Investments, ein auf NFT-Technologie spezialisiertes Inkubator-Unternehmen, Opfer eines Phishing-Angriffs von einer unbekannten externen Quelle. Der Angriff führte zu einem Verlust von 250.000 US-Dollar.[8]

Landratsamt Ludwigsburg: Im Mai 2023 griffen Cyber-Kriminelle das Landratsamt Ludwigsburg bei Stuttgart an. Infolgedessen musste das Amt geschlossen und vollständig abgeschaltet werden.[9]

Microsoft: Im Oktober 2023 zielte eine Phishing-Welle auf Microsoft-365-Konten in den USA ab. Ziel dieser Aktion waren Führungskräfte und hochrangige Mitarbeiter aus verschiedenen Branchen.[10]

Der Angriff auf das irische Gesundheitswesen (2021)

Im Jahr 2021 wurde die irische Gesundheitsbehörde (Health Service Executive, HSE) Opfer eines groß angelegten Ransomware-Cyberangriffs, der dazu führte, dass alle ihre IT-Systeme landesweit abgeschaltet werden mussten – während der Covid-Pandemie[11]. Es handelte sich um die weltweit größte bisher bekannte Sicherheitsverletzung in einem IT-System im Gesundheitswesen. Der Angriff wurde von einer russischen Verbrecherbande namens Wizard Spider durchgeführt.

Der Cyberangriff begann am 18. März 2021 mit einer Malware, die eine HSE-Arbeitsstation infizierte. Diese Infektion war möglich, weil der Benutzer dieses Arbeitsplatzes eine bösartige Microsoft Excel-Datei öffnete, die in einer Phishing-E-Mail enthalten war. Nachdem der Angreifer sich unbefugt Zugang zur IT-Umgebung der HSE verschafft hatte, bewegte er sich über einen Zeitraum von acht Wochen durch das Netzwerk. Er kompromittierte privilegierte Konten, infizierte zahlreiche Server und begann mit dem Exfiltrieren von Daten. Darüber hinaus weitete er den Angriff auf andere Systeme aus, darunter auch auf die IT-Umgebungen von Krankenhäusern, die der HSE angeschlossen sind.

5. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
6. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
7. https://portswigger.net/daily-swig/washington-residents-medical-data-exposed-by-phishing-attack-on-spokane-regional-health-district
8. https://www.proactiveinvestors.co.uk/companies/news/1003057/nft-investments-hit-by-us-250-000-phishing-attack-implements-incident-response-plan-1003057.html
9. https://www.heise.de/news/Cyber-Vorfaelle-beim-Verband-der-Pharmaindustrie-Kreis-Ludwigsburg-und-Sysco-9018251.html
10. https://www.bleepingcomputer.com/news/security/evilproxy-uses-indeedcom-open-redirect-for-microsoft-365-phishing/
11. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Dieses Whitepaper gibt einen umfassenden Überblick über Phishing-Angriffe und stellt Lösungen zu deren Bekämpfung vor. Wie gezeigt wird, bietet Eviden Digital Identity ein umfassendes Portfolio von Produkten zum Schutz vor Phishing.

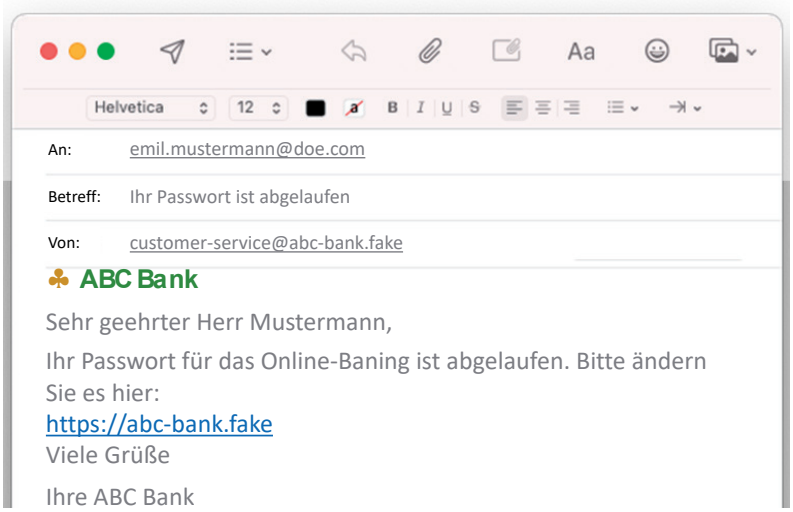
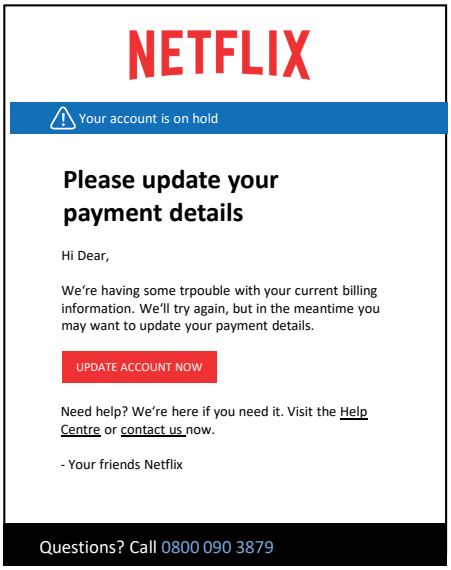
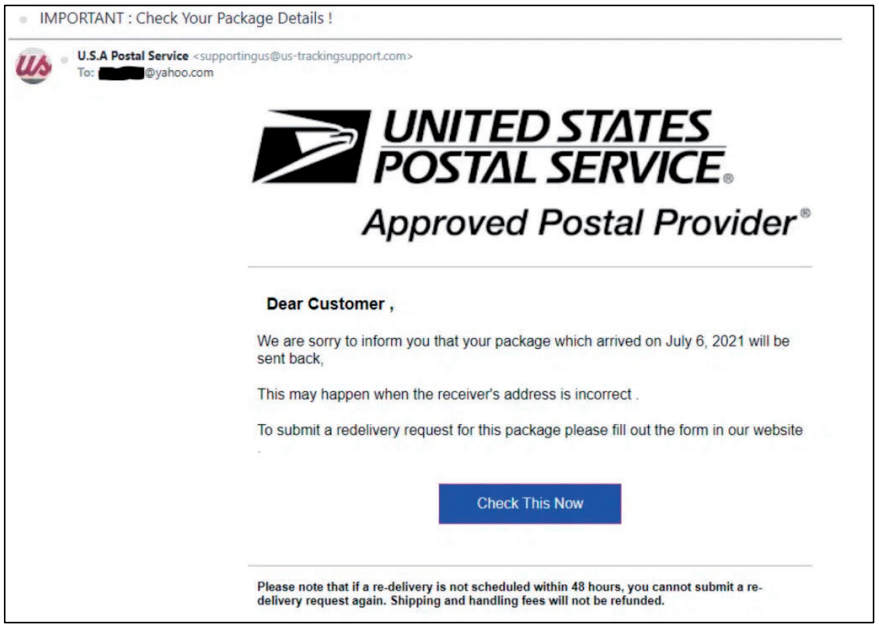


Abbildung 1: Ein Phishing-Angriff beginnt damit, dass der Angreifer eine gefälschte Nachricht mit einem falschen Link verschickt. Dies geschieht in der Regel per E-Mail oder Messenger.





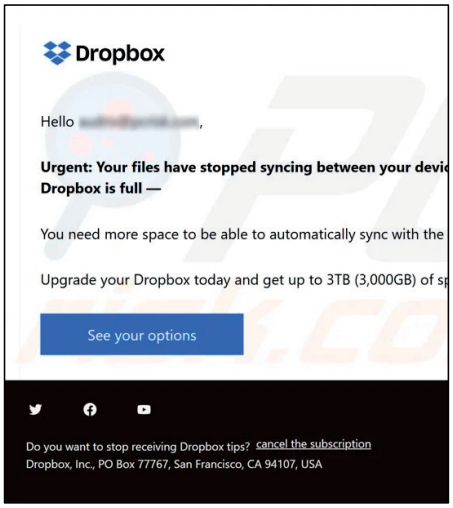


Abbildung 2: Viele Phishing-E-Mails sehen aus, als kämen sie von bekannten Unternehmen.

Bedrohung durch Phishing

So funktioniert Phishing

Ein Phishing-Angriff läuft in der Regel wie folgt ab:

1. Der Angreifer sendet eine gefälschte Nachricht mit einem Link zu einem betrügerischen Angebot (z. B. einer betrügerischen Webseite) an das Opfer. Dies geschieht in der Regel per E-Mail oder Messenger (siehe Abbildungen 1 und 2).
2. Das Opfer folgt dem Link.
3. Der betrügerische Server fordert das Opfer auf, ein Passwort oder sonstige Authentifizierungsdaten einzugeben.
4. Das Opfer gibt sein Passwort ein, ohne den Betrug zu bemerken.
5. Der betrügerische Server verwendet das erhaltene Passwort, um auf das Konto des Opfers auf dem echten Server zuzugreifen.

Die Erfolgswahrscheinlichkeit steigt, wenn die E-Mail aussieht, als stamme sie von einem bekannten Anbieter oder einem Arbeitskollegen. Da der Angreifer beim Phishing die zwischen zwei Parteien ausgetauschten Nachrichten manipuliert, handelt es sich um einen Man-in-the-Middle-Angriff.

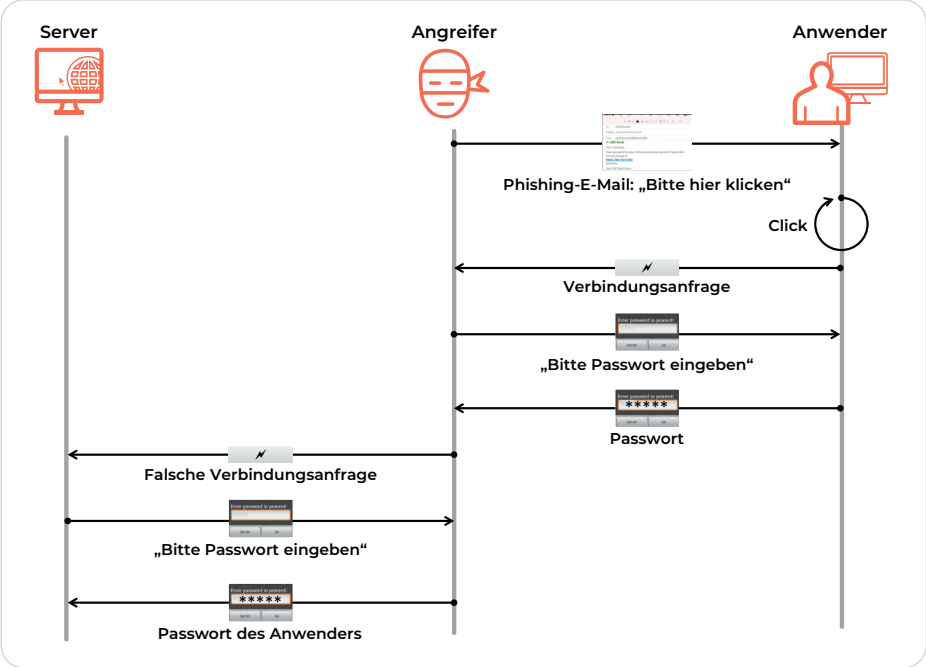


Abbildung 3: Beim Phishing werden Nachrichten manipuliert, die zwischen zwei Parteien ausgetauscht werden. Es handelt sich um einen Man-in-the-Middle-Angriff.

Aktuelle Trends

Phishing, eine seit den 1990er Jahren bekannte Technik, hat laut Forbes allein im Jahr 2022 mit über 500 Millionen gemeldeten Angriffen erheblichen Schaden angerichtet[12]. CNBC berichtet außerdem von einem Anstieg der Phishing-Angriffe zwischen Mai und Oktober 2022 um 61 % im Vergleich zum Vorjahr[13]. Vor allem in den USA gab es 2022 rund 300.497 Phishing-Opfer. Wie seriöse Quellen wie DIGIT NEWS („Phishing ist das wichtigste und am schnellsten wachsende Online-Verbrechen 2023")[14] CNBC („Phishing-Attacken nehmen zu und werden immer rafinierter")[15] und das Infosecurity Magazine („Phishing – Die Cybersecurity-Bedrohung des Jahres 2023")[16] berichten, werden Phishing-Angriffe immer raffinierter und bedrohen Unternehmen weltweit.

In letzter Zeit hat sich die künstliche Intelligenz (KI) zu einem wichtigen Werkzeug für die Vorbereitung und Durchführung von Phishing-Angriffen entwickelt. Ein Angreifer kann mithilfe von KI-Tools innerhalb kürzester Zeit Hunderttausende von maßgeschneiderten Phishing-Mails und gefälschten Webseiten erstellen. Aktuelle KI-Systeme sind in der Lage, grammatikalisch korrekte Texte in Dutzenden von Sprachen zu produzieren, die sowohl für Spam-Filter als auch für den Durchschnittsbürger schwer zu erkennen sind. Es wird erwartet, dass in naher Zukunft auch das Klonen von Stimmen und Gesichtern bei Phishing-Angriffen zum Einsatz kommt.

Insgesamt stellt Phishing eine erhebliche Bedrohung für Unternehmen und Behörden dar und führt zu Kosten, Datenverlusten und Rufschädigung.

12. https://www.forbes.com/advisor/business/phishing-statistics/
13. tinyurl.com/mryn2zz9
14. https://www.digit.fyi/phishing-the-most-dominant-and-fastest-growing-internet-crime-of-2023
15. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html
16. tinyurl.com/5emb7yny

Phishing-Methoden

Es gibt verschiedene Phishing-Varianten, darunter die folgenden:

- Spear-Phishing: Spear-Phishing ist eine gezielte Form des Phishings, bei der Cyber-Angreifer ihre betrügerischen Nachrichten so anpassen, dass sie für bestimmte Personen oder Organisationen besonders glaubhaft erscheinen. Dazu sind oft gründliche Nachforschungen über die beabsichtigten Opfer erforderlich.
- Vishing: Vishing oder Voice-Phishing ist eine Technik, bei der der Angreifer Telefonanrufe oder Sprachnachrichten verwendet, um das Opfer dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Aktionen durchzuführen. In der Regel geben sich Vishing-Angreifer als seriöse Organisationen wie Banken oder Behörden aus.
- Smishing: Smishing oder SMS-Phishing ist eine Technik, bei der der Angreifer SMS-Nachrichten verwendet, um Personen dazu zu verleiten, vertrauliche Informationen preiszugeben oder auf bösartige Links zu klicken. Diese betrügerischen Nachrichten geben sich oft als vertrauenswürdige Quellen, wie Banken oder Regierungsbehörden, aus.

In der Literatur werden zahlreiche weitere Varianten erwähnt.

Was NICHT gegen Phishing hilft

Authentifizierung ist ein wichtiges Werkzeug in der IT-Sicherheit. Es bezieht sich auf den Prozess der Überprüfung der Identität eines Benutzers, eines Geräts oder eines Systems, das versucht, auf eine bestimmte Ressource zuzugreifen. Diese Überprüfung erfolgt in der Regel durch die Vorlage eines Passworts, einer Smartcard oder biometrischer Daten. Die Authentifizierung dient als erste Verteidigungslinie gegen unbefugten Zugriff.

Man sollte beachten, dass es mehrere Techniken gibt, die einen Authentifizierungsprozess zwar sicherer machen, aber nicht gegen Phishing schützen. Einige davon sind im Folgenden aufgeführt:

- Sichere Passwörter: Schwer zu erratende Passwörter sind zwar wichtig, schützen aber nicht vor Phishing, da bei einem Phishing-Angriff das Passwort nicht erraten werden muss.
- Einmal-Passwörter (OTP) und SMS-Codes: Auch diese Techniken sind anfällig gegenüber Man-in-the-Middle-Angriffen und das Abfangen durch böswillige Akteure. Dennoch können OTPs, die auf einer Smartcard generiert werden, Teil einer Anti-Phishing-Strategie sein.
- Biometrische Authentifizierung gegenüber dem Server: Biometrische Methoden sind nicht immun gegen Man-in-the-Middle-Angriffe. Dennoch kann die biometrische Authentifizierung gegenüber der Smartcard Teil einer Anti-Phishing-Strategie sein.
- CAPTCHAs: Ein CAPTCHA ist zwar hilfreich, um Denial-of-Service-Angriffe zu verhindern, löst aber nicht das Problem der Man-in-the-Middle-Angriffe.

Gesetze und Vorschriften gegen Phishing

Die Erfahrung zeigt, dass es nicht ausreicht, Unternehmen und Behörden lediglich zu empfehlen, IT-Sicherheitsmaßnahmen zu ergreifen. Vielmehr bedarf es gesetzlicher Regelungen, die dies explizit fordern und bei Verstößen Strafen vorsehen.

Für Phishing relevante gesetzliche Regelungen gibt es bereits in vielen Ländern. Ein Beispiel ist die Netzwerk- und Informationssicherheitsrichtlinie (NIS2) der Europäischen Union, die Unternehmen und Behörden mit 50 oder mehr Mitarbeitern und einem Jahresumsatz von zehn Millionen Euro oder mehr betrifft. Unter anderem sieht NIS2 eine persönliche Haftung für Geschäftsführer und Vorstandsmitglieder vor, die bei Verstößen gegen die Cybersicherheitsverpflichtungen mit empfindlichen Geldstrafen belegt werden[17]. Phishing-Schutzmaßnahmen werden zwar nicht wörtlich erwähnt, gelten aber als unverzichtbares Mittel, um die Anforderungen von NIS2 zu erfüllen. Das Gleiche gilt für die EU-Datenschutzgrundverordnung (GDPR).

In Frankreich schreibt das LPM (Loi de Programmation Militaire), ein Gesetz, das die Verteidigungsstrategie des Landes, die militärischen Fähigkeiten und die Haushaltszuweisung für einen bestimmten Zeitraum festlegt, implizit einen Phishing-Schutz vor.

In Deutschland schreiben mehrere Gesetze implizit die Verwendung eines Phishing-Schutzes vor:

- Verschlusssachenanweisung: Diese deutsche Verordnung für Behörden und Anbieter kann nur erfüllt werden, wenn Maßnahmen zum Schutz vor Phishing getroffen werden[18].
- BSI-KritisV-Richtlinie: Gleiches gilt für diese Richtlinie, die auf die Sicherheit kritischer Infrastrukturen abzielt[19].
- IT-Sicherheitsgesetz 2.0: Dieses Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme verlangt implizit auch einen Phishing-Schutz.[20]

In den USA verlangt eine von Präsident Joe Biden am 12. Mai 2021 unterzeichnete Direktive des Weißen Hauses eine Phishing-resistente Authentifizierung für US-Behörden[21]. Sie besagt: „Agentursysteme müssen die Unterstützung für Authentifizierungsmethoden einstellen, die nicht gegen Phishing geschützt sind, wie z. B. Protokolle, die Telefonnummern für SMS- oder Sprachanrufe registrieren, einmalige Codes bereitstellen oder Push-Benachrichtigungen empfangen.“ Die Umstellung ist innerhalb von 180 Tagen erforderlich. Diejenigen, die die Frist bis zum 8. November nicht einhalten können, müssen alle 60 Tage Berichte vorlegen, bis sie die Phishing-sichere Authentifizierung vollständig eingeführt haben.

Da Phishing ein weltweites Phänomen ist, ist eine internationale Zusammenarbeit bei der Abwehr von Phishing erforderlich. Unternehmen haben die Pflicht, Phishing zu verhindern, um Kunden, Mitarbeiter, ihren Ruf und ihre finanzielle Stabilität zu schützen. Um dieser Verantwortung gerecht zu werden, sollten Unternehmen in die Cybersicherheit investieren und proaktive Maßnahmen zur Bekämpfung von Phishing-Angriffen ergreifen.

Zertifikatsbasierte Authentifizierung als Gegenmaßnahme

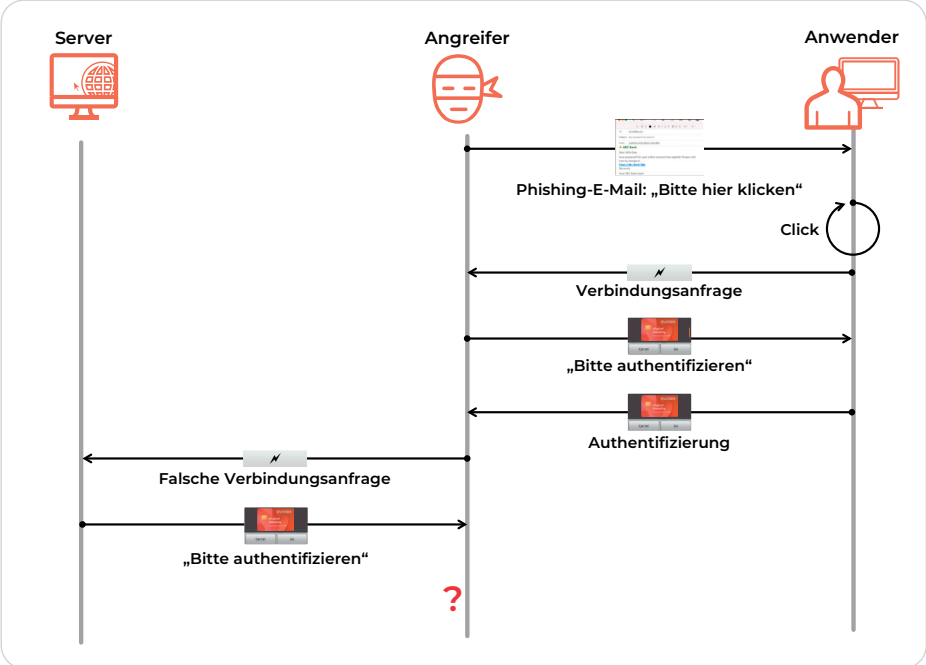


Abbildung 4: Die signaturbasierte Authentifizierung ist ein Challenge-Response-Mechanismus zur Bekämpfung von Phishing-Angriffen.

17. https://tinyurl.com/mr4cxmyd, https://tinyurl.com/5eath8fm
18. https://tinyurl.com/yc7fre76
19. https://www.gesetze-im-internet.de/bsi-kritisv/
20. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
21. https://www.yubico.com/blog/a-new-white-house-directive-phishing-resistance/

Signaturbasierte Authentifizierung

Die Authentifizierung auf der Grundlage digitaler Signaturen ist eine wichtige Maßnahme gegen Phishing. In der Regel wird ein Challenge-Response-Authentifizierungsprotokoll wie das folgende durchgeführt:

1. Der Server sendet eine Aufforderung an den Client. Die Aufforderung enthält eine Zufallszahl, die aktuelle Uhrzeit und die URL des Servers.
2. Der Client signiert die Challenge und sendet sie als Antwort an den Server zurück.
3. Der Server prüft die Signatur. Wenn sie korrekt ist und die Challenge unverändert bleibt, ist die Authentifizierung erfolgreich.

Zertifikats-basierte Authentifizierung

Die signaturbasierte Authentifizierung setzt voraus, dass der Server den öffentlichen Signaturschlüssel des Clients kennt. Natürlich kann dies erreicht werden, indem der Client seinen öffentlichen Signaturschlüssel mit der Antwort sendet, aber in diesem Fall ist der öffentliche Schlüssel möglicherweise nicht authentisch. Der naheliegendste Weg, die Authentizität des Schlüssels festzustellen, ist die Verwendung digitaler Zertifikate. In diesem Fall funktioniert das Authentifizierungsprotokoll wie folgt:

1. Der Server sendet eine Challenge (mit einer Zufallszahl, der aktuellen Uhrzeit und der URL des Servers) an den Server.
2. Der Client signiert die Challenge und sendet sie als Antwort an den Server zurück. Außerdem sendet er sein digitales Zertifikat, das seinen öffentlichen Schlüssel enthält.
3. Der Server prüft die Signatur und das digitale Zertifikat. Wenn alles korrekt ist, ist die Authentifizierung erfolgreich. Die zertifikatsbasierte Authentifizierung ist resistent gegen Phishing, da die Antwort die signierte URL des Servers enthält. Im Falle eines Phishing-Angriffs wird die URL des angreifenden Servers signiert. Wenn der Angreifer diese URL nicht ändert, wird der Server die Antwort nicht akzeptieren, da sie eine falsche URL enthält. Ändert der Angreifer die URL, akzeptiert der Server die Antwort nicht, da die Signatur falsch ist.

Um die Sicherheit zu erhöhen, kann die Technik des Token-Binding eingesetzt werden[22]. Das bedeutet, dass der Client nicht nur eine Challenge signiert, sondern auch einen Datensatz (Token), der seine Identität und möglicherweise andere Informationen wie eine URL enthält. Ein Token kann über mehrere Protokollsitzungen hinweg verwendet werden. Für einen Angreifer ist es praktisch unmöglich, ein Token zu fälschen, und es ist nutzlos, ein Token zu stehlen, da sich die enthaltenen Identitätsinformationen auf eine andere Instanz beziehen und nicht geändert werden können.

Infrastruktur für öffentliche Schlüssel (PKI)

Für die zertifikatsbasierte Authentifizierung muss eine Infrastruktur vorhanden sein, die die Ausstellung und Verteilung digitaler Zertifikate ermöglicht. Mit anderen Worten: eine Public-Key-Infrastruktur (PKI) ist erforderlich. In vielen Fällen kann eine bestehende Unternehmens-PKI verwendet werden. Wenn dies nicht der Fall ist, kann eine öffentliche Zertifizierungsstelle (CA) oder ein PKI-as-a-Service-Angebot genutzt werden. Es ist auch möglich, eine neue PKI aufzubauen und sie für die zertifikatsbasierte Authentifizierung sowie für andere Anwendungen zu nutzen.

Public-Key-Infrastrukturen sind eine bewährte Sicherheitstechnologie, die vor vielen verschiedenen Risiken schützt.

FIDO-Authentifizierung als Gegenmaßnahme

Anstelle einer PKI kann die FIDO-Authentifizierungsinfrastruktur für die Authentifizierung des öffentlichen Signaturschlüssels des Kunden verwendet werden. FIDO, die Abkürzung für „Fast Identity Online“, ist ein offener Industrieverband und eine Reihe von Standards und Protokollen, die die Online-Authentifizierung verbessern sollen. Die FIDO Alliance, die Organisation hinter FIDO, wurde gegründet, um die wachsenden Herausforderungen im Zusammenhang mit herkömmlichen passwortbasierten Authentifizierungsmethoden zu bewältigen, die oft anfällig für verschiedene Formen von Cyberangriffen, einschließlich Phishing, sind.

FIDO-Authentifizierung

Die FIDO-Authentifizierungsmethoden ermöglichen es jedem Benutzer, sein eigenes Schlüsselpaar für jeden von ihm verwendeten Server zu erzeugen. Auf der Grundlage dieses Schlüsselpaars wird die signaturbasierte Authentifizierung angewendet, wie oben beschrieben. Die FIDO-Methode ist zwar weniger sicher als digitale Zertifikate, lässt sich aber in Umgebungen, die keine PKI enthalten, leichter einsetzen. Im Gegensatz zu einer PKI kann die FIDO-Authentifizierung jedoch nicht auf digitale Signaturen, Verschlüsselung und verschiedene andere Authentifizierungsanwendungen, einschließlich VPN-Zugang, ausgeweitet werden.

Auch hier ist der Grund, warum dieses Verfahren Phishing-sicher ist, der, dass die URL des Servers Teil der signierten Nachricht ist. Auch Token-Binding, das die Sicherheit weiter erhöht, kann verwendet werden.

22. https://datatracker.ietf.org/doc/rfc8471/

FIDO-Infrastruktur

Die FIDO-Authentifizierung ist eine ausgereifte Technologie, die in verschiedenen Kontexten in der gesamten digitalen Landschaft eingesetzt wird, darunter Online-Dienste, Webseiten, Finanzdienstleistungen, Unternehmensauthentifizierung, Behördendienste, Gesundheitswesen, Cloud-Dienste, Bildung, IoT-Geräte, mobile Apps und plattformübergreifende Authentifizierung.

Die Akzeptanz der FIDO-Authentifizierung nimmt weiter zu, da Organisationen ihre Vorteile in Bezug auf Sicherheit, Benutzerfreundlichkeit und Datenschutz erkennen. Benutzer können die Vorteile von FIDO-kompatiblen Geräten und Authentifizierungsmethoden nutzen, um die Sicherheit ihrer Online-Konten und -Transaktionen zu verbessern.

Ende-zu-Ende-Schutz als Gegenmaßnahme

Eine sichere Authentifizierung durch digitale Signaturen ist nicht der einzige Ansatz zum Schutz vor Phishing. Eine weitere Möglichkeit besteht darin, Phishing-E-Mails zu verhindern.

Ende-zu-Ende-Schutz

Um eine E-Mail vor unbefugtem Lesen zu schützen, sollte man sie verschlüsseln. Moderne Verschlüsselungslösungen basieren auf asymmetrischer Kryptografie mit Algorithmen wie RSA oder Diffie-Hellman. Wer seine E-Mails darüber hinaus vor Manipulationen und Fälschungen schützen will, sollte digitale Signaturen einsetzen. Digitale Signaturen basieren ebenfalls auf asymmetrischer Kryptografie. Das Verschlüsseln und das digitale Signieren sind ähnliche Techniken, die leicht zusammen eingesetzt werden können.

Um E-Mails durch Kryptografie effektiv zu schützen, wird empfohlen, eine Ende-zu-Ende-Verschlüsselung und digitale Signaturen zu verwenden. Dies bedeutet, dass Verschlüsselung, Signierung, Entschlüsselung und Überprüfung direkt auf dem Computer des Benutzers durchgeführt werden.

Der kryptografische E-Mail-Schutz in einem Unternehmen sollte durch eine PKI unterstützt werden. Es ist zwar auch möglich, eine Out-of-Band-Schlüsselverteilung zu verwenden, doch ist dies nur für eine kleine Benutzergruppe ratsam. Natürlich kann dieselbe PKI für den E-Mail-Schutz und die zertifikatsbasierte Authentifizierung verwendet werden. Zertifikate können von einer internen PKI oder einem Drittanbieter – beispielsweise einer öffentlichen Zertifizierungsstelle oder einem PKI-as-a-Service-Betreiber, der auch cloudbasiert sein kann – genutzt werden.

Wie E-Mail-Signaturen und Verschlüsselung vor Phishing schützen

Digitale Signaturen schützen zuverlässig gegen Phishing-E-Mails. Wenn legitime E-Mails routinemäßig signiert werden, weiß ein Benutzer sofort, dass er einer unsignierten E-Mail nicht vertrauen darf.

Auch die Verschlüsselung von E-Mails erhöht die Sicherheit vor Phishing-Angriffen, da ein Angreifer den öffentlichen Schlüssel des Empfängers verwenden muss, um eine glaubwürdige E-Mail vorzutäuschen. Dies ist zwar möglich, erfordert aber einen zusätzlichen Schritt zur Erstellung einer Phishing-E-Mail, was das Phishing schwieriger macht. Außerdem funktionieren identische Phishing-Mails, die an Tausende von Empfängern geschickt werden, in einem solchen Fall nicht.

Insgesamt erhöhen das Signieren und das Verschlüsseln die E-Mail-Sicherheit in vielerlei Hinsicht. Der Schutz vor Phishing ist nur einer der vielen Vorteile, die diese Technologien bieten.

Einsatz

Die Einführung von kryptografischem E-Mail-Schutz erfordert ein Systemintegrationsprojekt. Für die Verwaltung der digitalen Zertifikate kann in vielen Fällen eine bestehende PKI genutzt werden. Darüber hinaus gibt es zahlreiche Anbieter von PKI-Diensten, einschließlich Cloud-basierter und PKI-as-a-Service-Lösungen. Das Verschlüsseln und Signieren von E-Mails wird seit über 20 Jahren in zahlreichen Unternehmen weltweit praktiziert. Es handelt sich um eine etablierte Technologie, deren Anwendungsbereich weit über den Schutz vor Phishing hinausgeht. In naher Zukunft werden PKIs mit Post-Quantum-Kryptoalgorithmen ausgestattet werden müssen, um sie gegen Quantencomputer-Angriffe zu schützen.

Eviden Digital Identity-Lösungen

Eviden ist ein Unternehmen mit den Geschäftsbereichen Digital, Cloud und Big Data & Security. Eviden, ein weltweit führender Anbieter von datengesteuerter, vertrauenswürdiger und nachhaltiger digitaler Transformation, ist ein digitales Unternehmen der nächsten Generation und verfügt über weltweit führende Positionen in den Bereichen Digital, Cloud, Daten, Advanced Computing und Sicherheit.

Eviden Digital Identity ist die Heimat der Lösungen cryptovision, CardOS und IDnomic, die entwickelt wurden, um elektronische Identitäten mit kryptografischen Lösungen und Anwendungen zu schützen.

Eviden Digital Identity bietet mehrere leistungsstarke Lösungen, die Phishing-Angriffe verhindern. Darüber hinaus umfasst das Eviden-Portfolio Produkte zur Implementierung von Einmal-Passwörtern, darunter CardOS SmartOTP und HOTP/TOTP. Diese Lösungen sind jedoch für die Abwehr von Phishing-Angriffen nicht relevant.

Zertifikatsbasierte Authentifizierung von Eviden

Eviden Digital Identity bietet ein Portfolio von Lösungen, die den Einsatz von zertifikatsbasierter Authentifizierung ermöglichen:

- CardOS: Dieses Chipkarten-Betriebssystem unterstützt sowohl FIDO als auch zertifikatsbasierte Authentifizierung.
- cryptovision ePasslet Suite: Die cryptovision ePasslet Suite ist ein Java Card-basiertes Framework für Smartcards, das FIDO-Token und zertifikatsbasierte Authentisierung unterstützt.
- cryptovision SCinterface: Diese Lösung stellt eine plattformunabhängige Middleware für die Nutzung von Smart Cards und Token dar. Sie enthält optionale Erweiterungen für Benutzerfreundlichkeit und Benutzerzufriedenheit, einschließlich VirtualSmatCard und RemoteSmartCard. Sie unterstützt zertifikatsbasierte Authentifizierung, digitale Signaturen und Verschlüsselung.
- IDnomic PKI: IDnomic PKI ist eine robuste und leistungsstarke mandantenfähige Zertifizierungsstellenlösung. Sie kann unter anderem für den Betrieb einer PKI für zertifikatsbasierte Authentifizierung und E-Mail-Schutz eingesetzt werden.
- IDnomic CMS: Das Credential Management System (CMS) von IDnomic verbessert die Verwaltung digitaler Zertifikate in einer PKI und erleichtert die globale Verwaltung kryptografischer Medien. Zu den unterstützten PKI-Anwendungen gehören zertifikatbasierte Authentifizierung und E-Mail-Schutz.
- IDnomic CLM: Diese Lösung für das Certificate Lifecycle Management (CLM) unterstützt eine Reihe hilfreicher Funktionen, die den Einsatz einer PKI insbesondere in heterogenen Umgebungen erleichtern. Davon können die zertifikatsbasierte Authentifizierung und der E-Mail-Schutz profitieren.
- IDnomic Sign: IDnomic Sign ermöglicht sichere digitale Signaturen, die unter anderem zum Phishing-Schutz eingesetzt werden können.
- Evidian Web Access Manager: Der Evidian Web Access Manager enthält einen Reverse-Proxy, der eine zentralisierte Authentifizierung ermöglicht. Es bietet eine Reihe starker Authentifizierungsmethoden, einschließlich zertifikatbasierter Authentifizierung und FIDO mit Token-Bindung. Nach der Authentifizierung erhalten Benutzer nur Zugriff auf Ressourcen, für die sie über entsprechende Berechtigungen verfügen. Dies trägt zum Schutz vor Phishing-Versuchen und unbefugtem Zugriff bei.

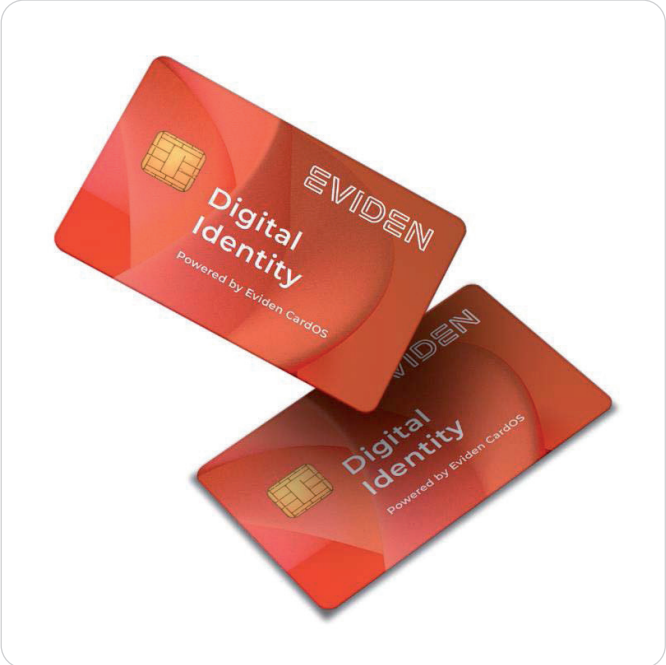


Abbildung 5: Das Smartcard-Betriebssystem CardOS unterstützt sowohl FIDO als auch zertifikatsbasierte Authentifizierung.

FIDO-Authentifizierung von Eviden

Die folgenden Eviden-Produkte unterstützen die FIDO-Authentifizierung:

- CardOS: Das Smartcard-Betriebssystem CardOS unterstützt sowohl die FIDO-Token- als auch die zertifikatsbasierte Authentifizierung (letztere wird durch die Verwendung des SCinterface ePKI-Applets erreicht). Es stehen zwei Formfaktoren zur Verfügung: ein Token mit USB- und NFC-Schnittstelle sowie eine traditionelle Chipkarte mit kontaktbehafteter und kontaktloser Schnittstelle. CardOS FIDO2 ist eine FIDO-zertifizierte Anwendung für CardOS-Chipkarten, um diese als FIDO-Authentifikator zu verwenden.
- Evidian Web Access Manager: Der Evidian Web Access Manager unterstützt eine Reihe von starken Authentifizierungsmethoden, einschließlich zertifikatsbasierter Authentifizierung und FIDO mit Token-Bindung.

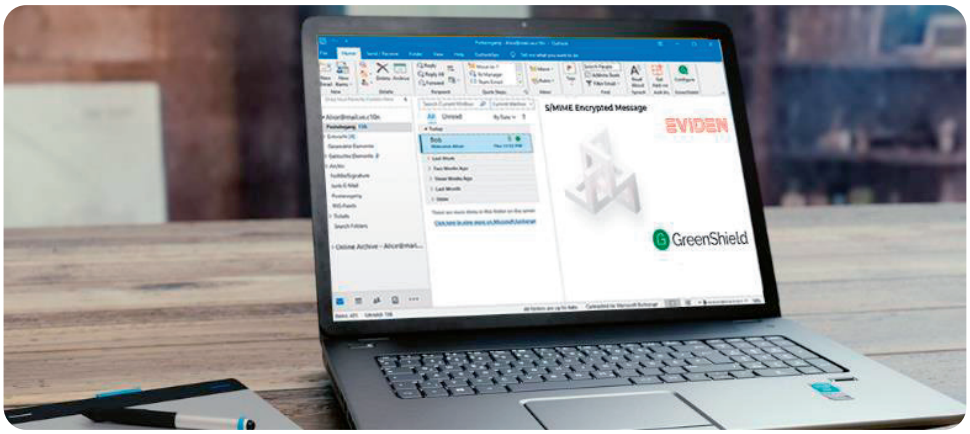


Abbildung 6: cryptovision GreenShield bietet durchgängigen E-Mail- und Dateischutz integriert in Outlook und Notes.

Kryptografischer E-Mail-Schutz von Eviden

Eviden bietet mehrere leistungsstarke Tools für den E-Mail-Schutz:

- Cryptovision GreenShield: cryptovision GreenShield bietet eine nahtlos in Microsoft Outlook und HCL (Lotus) Notes integrierte Ende-zu-Ende E-Mail- und Dateiverschlüsselung/Signatur. Cryptovision GreenShield ist zugelassen für VS-NfD, NATO-, EU- und EU-Verschlusssachen.
- Cryptovision GreenShield Comfort: Hierbei handelt es sich um eine Komplettlösung, die eine Ende-zu-Ende-Verschlüsselung, PKI-Dienste sowie ein durch automatisierte Workflows gesteuertes Schlüssel- und Zertifikats-Lifecycle-Management bietet.

Der Schutz vor Phishing ist nur eines von mehreren Zielen, die mit diesen Lösungen erreicht werden können.

Eviden-Referenzen

Eviden Digital Identity verfügt über zwei Jahrzehnte Erfahrung mit zertifikatsbasierter Authentifizierung, PKI und Ende-to-Ende-E-Mail-Verschlüsselung. In der folgenden Liste sind einige Kunden aufgeführt:

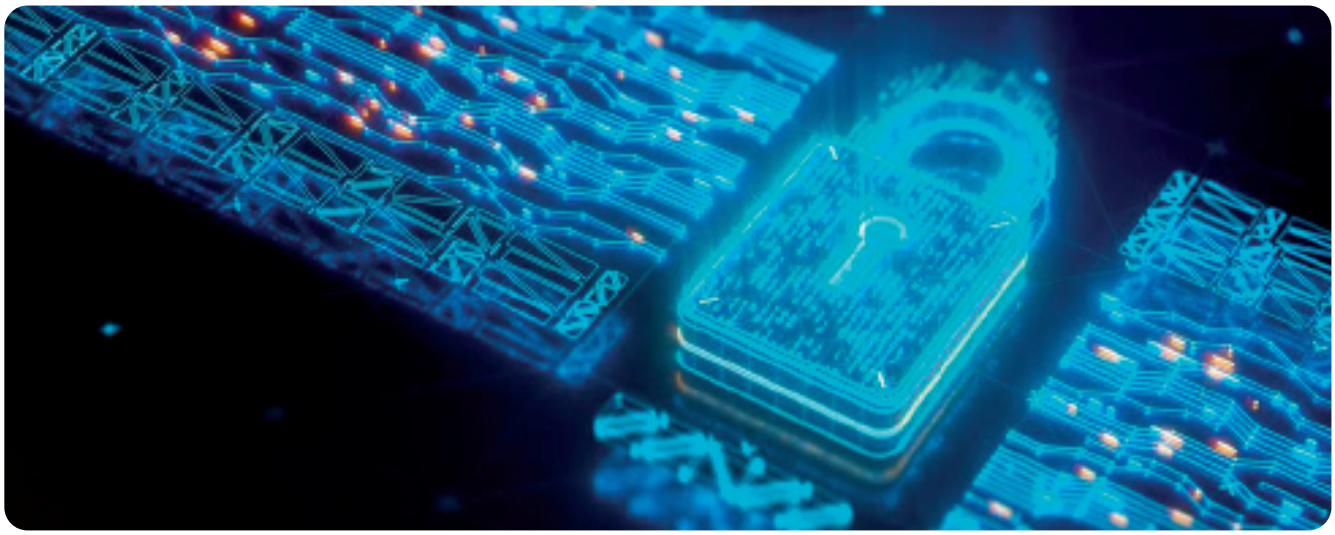
- ADAC: Zertifikatsbasierte Authentifizierung
- Airbus: PKI-Lösung
- Allianz: Zertifikatsbasierte Authentifizierung, digitale Signatur und PKI-Lösung
- BNP Paribas: PKI-Lösung
- Bouygues Telecom: PKI-Lösung
- Bundesministerium für Finanzen: Sichere E-Mail und PKI-Lösung
- Bundesministerium für Bildung und Forschung: Sichere E-Mail und PKI-Lösung
- Bundeswehr: E-Mail-Sicherheit mit cryptovision GreenShield Mail
- City of New York: PKI-Lösung
- Credit Agricole: PKI-Lösung
- Deutsche Telekom: Datei-Verschlüsselung
- e.on: Zertifikatsbasierte Authentifizierung und digitale Signatur
- EDF: PKI-Lösung
- European Commission: IDnomic PKI für intelligente Transportsysteme
- European Patent Office: Zertifikatsbasierte Authentifizierung und digitale Signatur
- Ministère de la Santé et de la Prévention: PKI-Lösung
- Ministère de l'Éducation nationale: PKI-Lösung
- Postbank: PKI-Lösung
- SAP: Sichere E-Mail

Warum Investitionen in Anti-Phishing-Technologien so wichtig sind

Phishing-Angriffe dienen oft als Einstiegspunkt für böswillige Akteure, um das Netzwerk eines Unternehmens zu kompromittieren. Die Investition in Phishing-resistente Technologien schützt daher die digitalen Werte und das geistige Eigentum eines Unternehmens.

Wenn ein Unternehmen Opfer eines Phishing-Angriffs wird, setzt es sich nicht nur unmittelbaren finanziellen und betrieblichen Risiken aus, sondern schadet auch seinem Ruf. Wenn Kundendaten kompromittiert oder Dienstleistungen unterbrochen werden, wird das Vertrauen untergraben, und die Kunden suchen möglicherweise nach Alternativen.

Die rechtlichen Rahmenbedingungen für den Datenschutz und die Cybersicherheit entwickeln sich ständig weiter. Zahlreiche Datenschutzgesetze und -vorschriften wie die Datenschutz-Grundverordnung, der Health Insurance Portability and Accountability Act (HIPAA) und der California Consumer Privacy Act (CCPA) stellen strenge Anforderungen an Unternehmen, um sensible Informationen vor unbefugtem Zugriff oder Offenlegung zu schützen. Die Nichteinhaltung dieser Vorschriften kann schwerwiegende finanzielle Strafen und rechtliche Konsequenzen nach sich ziehen. Die Investition in phishing-sichere Technologien hilft nicht nur bei der Einhaltung der Vorschriften, indem sie den unbefugten Zugriff auf sensible Daten verhindert, sondern zeigt auch, dass ein Unternehmen seinen gesetzlichen Verpflichtungen nachkommen will. Diese proaktive Haltung kann dazu beitragen, kostspielige rechtliche Verwicklungen und Bußgelder zu vermeiden.



Zusammenfassung

Zusammenfassend lässt sich sagen, dass Phishing-Angriffe eine erhebliche Gefahr für Unternehmen aller Größen und Branchen darstellen. Durch Investitionen in moderne, Phishing-resistente Technologien können Unternehmen die Risiken erheblich reduzieren, ihre Vermögenswerte schützen, einen tadellosen Ruf aufrechterhalten, das Vertrauen ihrer Kunden gewinnen und rechtliche Verpflichtungen erfüllen. Im ständigen Kampf gegen Cyber-Bedrohungen spielen diese Technologien eine entscheidende Rolle bei der Stärkung des digitalen Schutzes moderner Unternehmen und gewährleisten eine sichere, robuste und gesetzeskonforme Zukunft.

Eviden Digital Identity bietet eine Reihe von Produkten und Strategien, die Unternehmen einsetzen können, um ihre Widerstandsfähigkeit gegen die allgegenwärtige Bedrohung durch Phishing-Angriffe zu verbessern. Um mehr über unser Angebot zu erfahren, kontaktieren Sie uns bitte hier:

cv-info@eviden.com

www.cryptovision.com

Unser Beratungsteam setzt sich gerne mit Ihnen in Verbindung.

Eviden
cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

EVIDEN

Eviden[1]

Eviden ist ein Technologieunternehmen der nächsten Generation im Bereich der datengesteuerten, vertrauenswürdigen und nachhaltigen digitalen Transformation mit einem starken Portfolio an patentierten Lösungen. Mit weltweit führenden Positionen in den Märkten für Advanced Computing, Sicherheit, KI, Cloud und digitale Plattformen bietet Eviden fundiertes Fachwissen für alle Branchen in mehr als 47 Ländern. Eviden vereint 53.000 Talente und erweitert die Möglichkeiten von Daten und Technologien über das gesamte digitale Kontinuum hinweg, heute und für kommende Generationen. Eviden ist ein Unternehmen der Atos-Gruppe mit einem Jahresumsatz von ca. 5 Mrd. €.

[1] Eviden ist mit den folgenden Marken vertreten: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden ist eine eingetragene Marke. © Eviden SAS, 2023.

Atos

Atos ist ein weltweit führendes Unternehmen im Bereich der digitalen Transformation mit 105.000 Mitarbeitern und einem Jahresumsatz von ca. 11 Mrd. EUR. Als europäische Nummer eins in den Bereichen Cybersicherheit, Cloud und High-Performance Computing bietet die Gruppe maßgeschneiderte End-to-End-Lösungen für alle Branchen in 69 Ländern. Als Pionier bei Dienstleistungen und Produkten zur Dekarbonisierung setzt sich Atos für eine sichere und dekarbonisierte digitale Welt für seine Kunden ein. Atos ist eine SE (Societas Europaea) und an der Euronext Paris notiert.

Das Ziel von Atos ist es, die Zukunft des Informationsraums mitzugestalten. Seine Kompetenzen und Dienstleistungen unterstützen die Entwicklung von Wissen, Bildung und Forschung in einem multikulturellen Ansatz und tragen zur Entwicklung wissenschaftlicher und technologischer Spitzenleistungen bei. Weltweit ermöglicht die Gruppe ihren Kunden und Mitarbeitern sowie den Mitgliedern der Gesellschaft insgesamt, in einem sicheren und geschützten Informationsraum zu leben, zu arbeiten und sich nachhaltig zu entwickeln.

In den sozialen Medien

eviden.com

 20231213