EVIDEN

Développer la résilience

Solutions techniques contre le Phishing

Synthèse

Les attaques par hameçonnage sont devenues l'une des formes de cybercriminalité les plus répandues et les plus dynamiques de ces dernières années. Ces tentatives malveillantes consistent à tromper les utilisateurs de technologies de l'information pour qu'ils révèlent des informations sensibles, généralement par le biais de courriels ou de messages trompeurs menant à des sites web frauduleux. Plusieurs incidents très médiatisés, tels que la violation de SolarWinds[1] et le piratage de Colonial Pipeline[2], ont mis en évidence la gravité du problème. Le phishing est devenu une menace sophistiquée et l'utilisation de l'intelligence artificielle l'a rendue encore plus difficile à combattre. Les attaques par hameçonnage impliquent généralement qu'un attaquant envoie un message trompeur avec un lien contrefait, souvent en imitant des fournisseurs ou des collègues bien connus.

Les incidents d'hameçonnage se sont multipliés, avec plus de 500 millions d'attaques signalées en 2022[3], et une augmentation de 61 % des attaques entre mai et octobre 2022[4]. En particulier, les États-Unis ont enregistré environ 300 497 victimes de phishing en 2022. Plusieurs lois en France, en Allemagne et dans d'autres pays exigent implicitement une protection contre le phishing pour lutter contre cette menace. Si les mots de passe sécurisés, les mots de passe à usage unique (OTP), l'authentification biométrique et les CAPTCHA renforcent la sécurité, ils n'empêchent pas les attaques par hameçonnage. L'authentification par certificat, soutenue par une infrastructure à clé publique (ICP, PKI en anglais), est une contre-mesure efficace contre le phishing. Cette technologie permet de vérifier l'authenticité de la clé de signature publique du client, ce qui rend les tentatives d'hameçonnage beaucoup plus difficiles.

Au lieu d'une PKI et de certificats numériques, la solution alternative « Fast Identity Online » (FIDO) peut être utilisée pour authentifier la clé de signature publique du client utilisée pour la protection contre l'hameçonnage. Cette solution est particulièrement intéressante si aucune PKI n'est disponible. L'authentification par certificat et l'authentification FIDO sont encore plus sûres si l'on utilise la liaison par jeton. La protection cryptographique de bout en bout du courrier électronique, y compris l'utilisation du cryptage et des signatures numériques, est une autre technologie importante qui protège contre le phishing. Elle renforce la sécurité du courrier électronique et permet difficilement aux attaquants de se faire passer pour des expéditeurs légitimes.

Eviden offre une gamme de solutions de sécurité puissantes pour prévenir les attaques de phishing, y compris l'authentification basée sur des certificats et l'authentification FIDO avec token associé, ainsi que la protection cryptographique des courriels. Les plus importantes de ces solutions sont le système d'exploitation CardOS, IDnomic PKI (y compris une offre PKI-as-a-service basée sur le cloud) et cryptovision GreenShield. Les organisations sont encouragées à contacter Eviden pour discuter de leurs besoins spécifiques.

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

Introduction

Introduction

Les attaques par hameçonnage sont des tentatives malveillantes visant à tromper les utilisateurs des technologies de l'information et à leur faire révéler leurs identifiants de connexion ou d'autres informations sensibles. Il s'agit généralement de courriels ou de messages trompeurs qui conduisent les destinataires vers des sites web frauduleux. Ces dernières années, le paysage numérique a connu une augmentation alarmante des attaques par hameçonnage, ce qui en fait l'un des cybercrimes les plus dominants et à la croissance la plus rapide d'aujourd'hui. De nombreux exemples de failles de sécurité dues à l'hameçonnage ont été couverts par les médias (voir encadrés ci-contre).

Les failles de sécurité liées au Phishing

Voici quelques-unes des failles de sécurité les plus dévastatrices dues à l'hameçonnage :

SolarWinds : La faille de sécurité de SolarWinds, découverte en décembre 2020, est une cyberattaque sophistiquée qui a touché plusieurs agences gouvernementales américaines et organisations du secteur privé. Des pirates informatiques ont inséré un code malveillant dans une mise à jour du logiciel de la plateforme Orion de SolarWinds, un outil de surveillance de réseau très répandu. Lorsque les clients ont installé cette mise à jour compromise, elle a permis aux pirates d'obtenir un accès non autorisé à leurs réseaux. L'attaque a commencé par le piratage d'un compte. À partir de ce point d'ancrage initial, les attaquants ont pu envoyer des courriels d'hameçonnage pour inciter les victimes à cliquer sur un lien qui déploierait un cheval de Troie à porte dérobée. Le préjudice financier causé par la faille de sécurité de SolarWinds a été estimé à environ 90 millions de dollars.[5]

Colonial Pipeline : Le piratage de Colonial Pipeline s'est produit en mai 2021 et a consisté en une attaque par ransomware contre l'un des plus grands oléoducs des États-Unis. Les attaquants ont crypté les données de l'oléoduc et ont demandé une rançon en échange de la clé de décryptage. Là encore, le piratage a commencé par une attaque par hameçonnage.[6]

Agence de santé de l'État américain : En février 2022, les données médicales sensibles de plus de 1 200 résidents américains ont été exposées à la suite d'une attaque par hameçonnage réussie contre une agence de santé de l'État de Washington.[7]

NFT Investments : En janvier 2023, NFT Investments, un incubateur spécialisé dans la technologie NFT, a été victime d'une attaque par hameçonnage provenant d'une source externe inconnue. L'attaque a entraîné la perte de 250 000 dollars.[8]

District de Ludwigsburg : En mai 2023, des cybercriminels ont attaqué l'administration du district de Ludwigsburg en Allemagne. En conséquence, le bureau du district a dû être fermé et complètement mis hors service.[9]

Microsoft : En octobre 2023, une nouvelle campagne de phishing a visé les comptes Microsoft 365 aux États-Unis. Les cibles de cette campagne d'hameçonnage étaient des cadres et des employés de haut rang de diverses industries.[10]

Attaque contre le Irish Health Service Executive

En 2021, le Health Service Executive (HSE) d'Irlande a subi une importante cyberattaque par ransomware, qui a entraîné l'arrêt de tous ses systèmes informatiques à l'échelle nationale pendant la pandémie de Covid[11]. Il s'agit de la plus grande atteinte à la sécurité d'un système informatique d'un service de santé jamais connue en histoire. L'attaque a été menée par un gang criminel russe connu sous le nom de Wizard Spider.

La cyberattaque a débuté le 18 mars 2021 par l'infection d'un poste de travail du HSE par un logiciel malveillant. Cette infection a été possible parce que l'utilisateur de ce poste de travail a ouvert un fichier Microsoft Excel malveillant qui était inclus dans un courriel d'hameçonnage. Après avoir obtenu un accès non autorisé à l'environnement informatique du HSE, l'attaquant s'est déplacé sur le réseau pendant huit semaines. Il a promis des comptes privilégiés, infecté de nombreux serveurs et commencé à exfiltrer des données. En outre, il a étendu l'attaque à d'autres systèmes, y compris les environnements informatiques des hôpitaux affiliés au HSE.

Pendant des semaines, les administrateurs informatiques du HSE n'ont pas réagi à plusieurs signaux d'alarme indiquant qu'une attaque massive était imminente. L'incident n'a été détecté que lorsque le ransomware Conti est devenu actif le 14 mai 2021 et a provoqué une perturbation informatique généralisée en chiffrant les données. L'attaque a entraîné un arrêt presque complet des réseaux nationaux et locaux du HSE et une interruption de service dans plusieurs cliniques et services de santé. Le nombre de rendez-vous a diminué de 80 %.

Le groupe Conti a d'abord exigé une rançon de 20 millions de dollars en crypto-monnaie en échange de la clé numérique permettant de décrypter les serveurs HSE compromis. Après que l'affaire a été rendue publique et que le public s'est insurgé, le groupe Conti a remis gratuitement les clés de décryptage au HSE.

Le coût de la récupération est estimé à environ 530 millions d'euros. Les informations médicales d'au moins 520 patients, ainsi que des documents d'entreprise ont été publiés en ligne.

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

Ce livre blanc a pour but de fournir une vue d'ensemble des attaques de phishing et des solutions efficaces pour les combattre. Comme nous le verrons, Eviden Digital Identity offre une suite complète de produits avancés pour renforcer la résilience face au phishing.

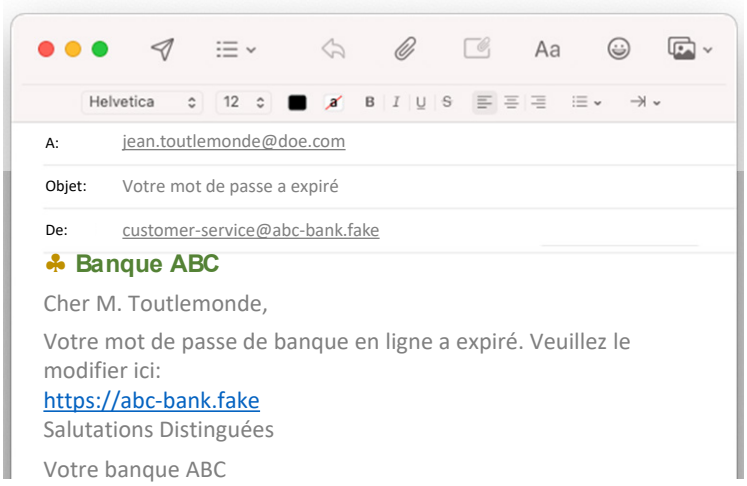


Figure 1: Une attaque par hameçonnage commence par l'envoi par l'attaquant d'un message trompeur contenant un lien contrefait. Ce message est généralement envoyé par courrier électronique ou par messagerie instantanée.

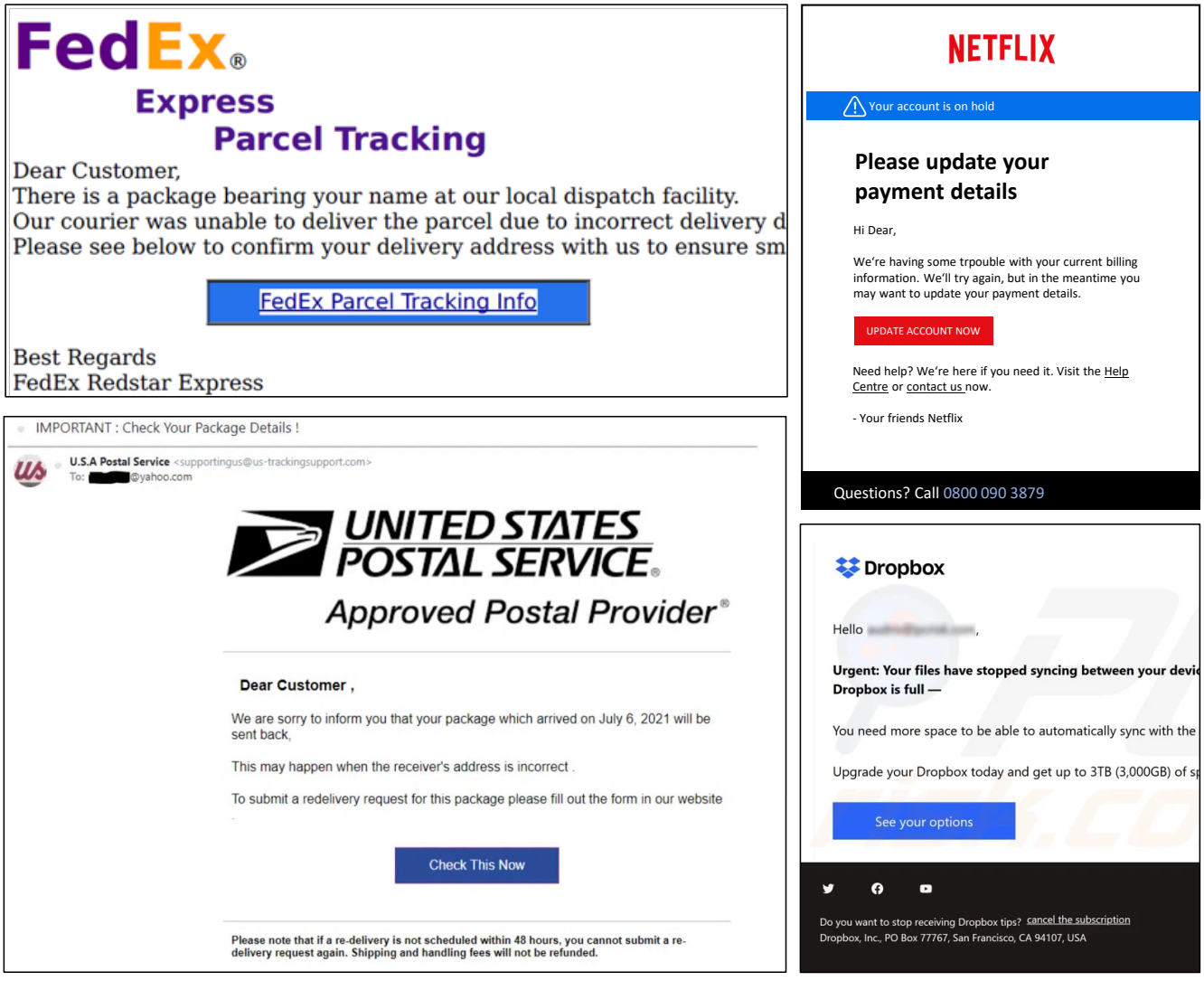


Figure 2: De nombreux courriels de phishing semblent provenir d'entreprises connues.

L‘hameçonnage, un scénario de plus en plus menaçant

Comment fonctionne le Phishing ?

Une attaque par hameçonnage comporte généralement les étapes suivantes :

1. L‘attaquant envoie à la victime un faux message contenant un lien contrefait. Cette opération s‘effectue généralement par courrier électronique ou par messagerie (voir figures 1 et 2).
2. La victime suit involontairement le lien, qui mène à un faux serveur (par exemple, un site web frauduleux).
3. Le faux serveur invite la victime à saisir des informations d‘authentification, telles qu‘un mot de passe.
4. La victime, ignorant la ruse, saisit son mot de passe.
5. Le faux serveur utilise alors le mot de passe obtenu pour accéder au compte de la victime sur le serveur authentique.

La probabilité de réussite augmente si le courriel semble provenir d‘un fournisseur ou d‘un collègue de travail bien connu. Comme l‘hameçonnage implique que l‘attaquant manipule les messages échangés entre deux parties, il appartient à la famille des attaques de type „man-in-the-middle“.

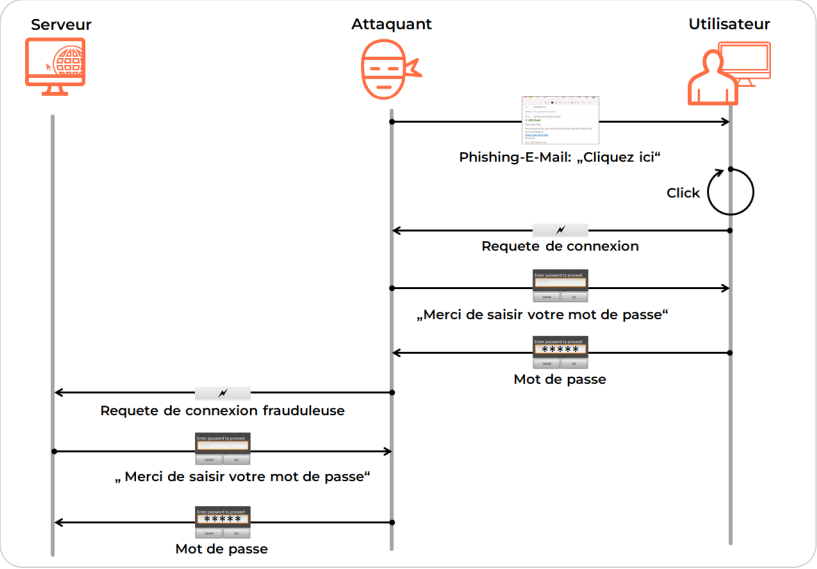


Figure 3: Le phishing consiste à manipuler les messages échangés entre deux parties. Il s‘agit d‘une attaque « man-in-the-middle ».

Statistiques et tendances

Le phishing, technique connue depuis les années 1990, a causé des dégâts considérables avec plus de 500 millions d‘attaques signalées pour la seule année 2022, selon Forbes[12]. CNBC rapporte également une augmentation de 61% des attaques de phishing entre mai et octobre 2022 par rapport à l‘année précédente[13]. En particulier, les États-Unis ont enregistré environ 300 497 victimes d‘hameçonnage en 2022.

Comme le soulignent des sources réputées telles que DIGIT NEWS ("Phishing the Most Dominant and Fastest Growing Internet Crime of 2023")[14], CNBC („Phishing attacks are increasing and getting more sophisticated“)[15], et Infosecurity Magazine („Phishing - The 2023 Cybersecurity Threat“)[16], les attaques de phishing sont devenues de plus en plus sophistiquées et représentent une menace substantielle pour les organisations du monde entier.

Récemment, l‘intelligence artificielle (IA) est devenue un moyen important de préparer et de mener des attaques de phishing. Un attaquant peut utiliser des outils d‘IA pour créer des centaines de milliers de courriers de phishing sur mesure et de faux sites web dans un court laps de temps. Les systèmes d‘IA actuels sont capables de produire des textes grammaticalement corrects dans des dizaines de langues qui sont difficiles à comprendre pour les filtres anti-spam et pour le citoyen moyen. Dans un avenir proche, le clonage de la voix et du visage devrait également jouer un rôle important dans les attaques de phishing.

Dans l‘ensemble, le phishing représente une menace importante pour les organisations, entraînant des pertes financières, des violations de données et des atteintes à la réputation.

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

Les différentes méthodes de Phishing

Il existe plusieurs variantes de phishing, dont les suivantes :

- **Le “Spear-phishing”** : Le spear-phishing est une forme ciblée d‘hameçonnage dans laquelle les cyber-attaquants personnalisent leurs messages trompeurs pour qu‘ils semblent très pertinents pour des personnes ou des organisations spécifiques. Cela implique souvent des recherches approfondies sur les victimes visées.
- **Le “Vishing”** : L‘hameçonnage vocal (« voice phishing ») est une technique dans laquelle l‘attaquant utilise des appels téléphoniques ou des messages vocaux pour inciter la victime à révéler des informations sensibles ou à entreprendre certaines actions. Généralement, les escroqueries par hameçonnage vocal consistent à se faire passer pour des organisations légitimes, telles que des banques ou des agences gouvernementales.
- **Le “Smishing”** : L‘hameçonnage par SMS (SMS phishing) est une technique de cyberattaque dans laquelle l‘attaquant utilise des messages textuels pour inciter des personnes à divulguer des informations sensibles ou à cliquer sur des liens malveillants. Ces messages trompeurs se font souvent passer pour des sources fiables, comme des banques ou des agences gouvernementales.

De nombreuses autres variantes sont mentionnées dans la littérature, mais ce document n‘a pas pour objet de les présenter toutes.

Techniques qui ne permettent pas de lutter contre le phishing

L‘authentification est un concept fondamental de la sécurité informatique. Elle fait référence au processus de vérification de l‘identité d‘un utilisateur, d‘un appareil ou d‘un système qui tente d‘accéder à une ressource spécifique. Cette vérification s‘effectue généralement par la présentation d‘un mot de passe, d‘une carte à puce ou de données biométriques. L‘authentification constitue la première ligne de défense contre les accès non autorisés. Il est important de noter qu‘il existe plusieurs techniques qui rendent les processus d‘authentification plus sûrs, mais qui n‘empêchent pas l‘hameçonnage. Certaines d‘entre elles sont énumérées ci-dessous:

- **Mots de passe sécurisés** : Les mots de passe difficiles à deviner, bien qu‘importants, ne protègent pas contre l‘hameçonnage, car une attaque par hameçonnage n‘implique pas de deviner le mot de passe.
- **Mots de passe à usage unique (OTP) et codes SMS** : Ces techniques sont également sujettes à des attaques de type „man-in-the-middle“ et à l‘interception par des acteurs malveillants. Néanmoins, les OTP, générés sur une carte à puce, peuvent faire partie d‘une stratégie anti-phishing.
- **Authentification biométrique contre le serveur** : Les méthodes biométriques ne sont pas à l‘abri des attaques de type „man-in-the-middle“. Cependant, l‘authentification biométrique contre la carte à puce peut faire partie d‘une stratégie anti-phishing.
- **CAPTCHAs** : Un CAPTCHA, bien qu‘utile pour prévenir les attaques par déni de service, ne résout pas le problème des attaques de type « man-in-the-middle ».

Cadres juridiques

L'expérience a montré qu'il ne suffit pas de recommander aux entreprises et aux autorités de mettre en œuvre des mesures de sécurité informatique. Il faut au contraire des réglementations légales qui l'exigent explicitement et imposent des sanctions en cas de non-respect.

Dans de nombreux pays, il existe déjà des réglementations légales concernant le phishing. Un exemple est la directive sur la sécurité des réseaux et de l'information (NIS2) de l'Union européenne, qui concerne les entreprises et les autorités publiques employant 50 personnes ou plus et dont le chiffre d'affaires annuel est supérieur ou égal à dix millions d'euros. Entre autres, la directive NIS2[17] introduit une responsabilité personnelle pour les directeurs généraux et les membres du conseil d'administration, qui devront s'acquitter d'amendes élevées en cas de manquement aux obligations en matière de cybersécurité. La résilience au phishing, bien qu'elle ne soit pas mentionnée littéralement, est considérée comme un moyen indispensable pour satisfaire aux exigences de la NIS2. Il en va de même pour le règlement général sur la protection des données (RGPD) de l'UE.

En France, la LPM (Loi de Programmation Militaire) est un texte législatif qui définit la stratégie de défense du pays, les capacités militaires et l'allocation budgétaire pour une période donnée, exige implicitement une protection contre le phishing.

En Allemagne, plusieurs lois exigent implicitement l'utilisation d'une protection contre l'hameçonnage :

- **« Verschlusssachenanweisung »** : Ce règlement allemand destiné aux autorités et aux fournisseurs ne peut être respecté que si des mesures de protection contre les phishings sont mises en œuvre.[18]
- **« Directive BSI KritisV »** : Il en va de même pour cette directive visant la sécurité des infrastructures critiques.[19]
- **« IT-Sicherheitsgesetz 2.0 »** : Cette loi visant à accroître la sécurité des systèmes de technologie de l'information exige implicitement une protection contre l'hameçonnage.[20]

Aux États-Unis, une directive de la Maison Blanche signée par le président Joe Biden le 12 mai 2021 impose aux agences américaines une authentification résistante au phishing[21] : „Les systèmes des agences doivent cesser de prendre en charge les méthodes d'authentification qui ne résistent pas au phishing, comme les protocoles qui enregistrent des numéros de téléphone pour les SMS ou les appels vocaux, qui fournissent des codes à usage unique ou qui reçoivent des notifications push." La migration est requise dans un délai de 180 jours. Ceux qui ne pourront pas respecter la date limite du 8 novembre devront fournir des rapports tous les 60 jours jusqu'à ce qu'ils aient entièrement déployé l'authentification résistante au phishing.

Le phishing étant un phénomène mondial, une collaboration internationale est nécessaire pour s'en défendre. Les entreprises ont la responsabilité de prévenir le phishing afin de protéger leurs clients, leurs employés, leur réputation et leur stabilité financière. Pour s'acquitter de cette responsabilité, les entreprises doivent investir dans la cybersécurité et prendre des mesures proactives pour lutter contre les attaques de phishing.

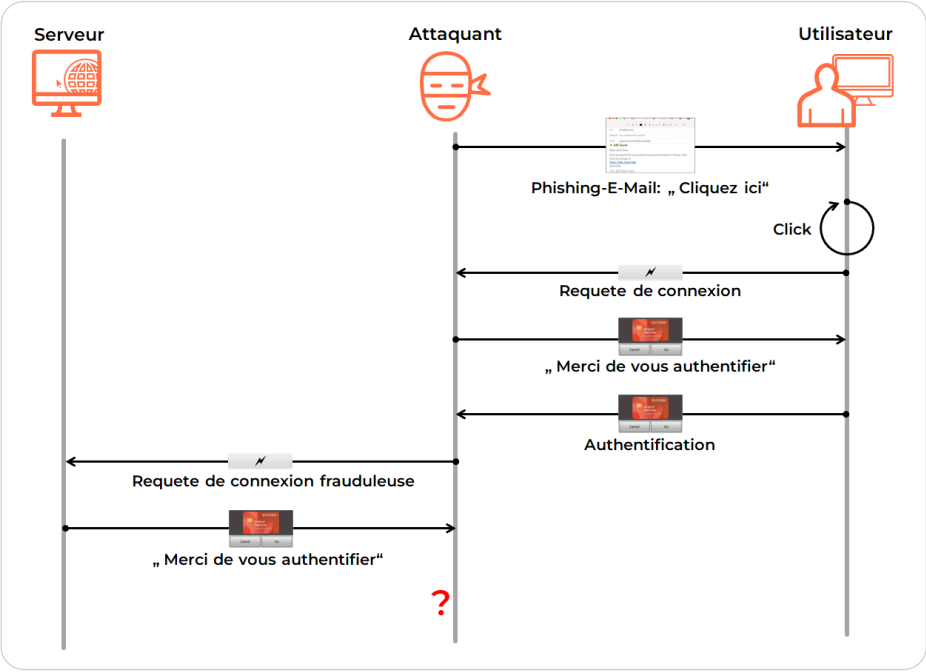


Figure 4: L'authentification basée sur la signature est un mécanisme de défi/réponse qui permet de lutter contre les attaques par hameçonnage.

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/

L‘authentification par certificat

Authentification basée sur la signature

L‘authentification basée sur la signature numérique est une contre-mesure importante contre l‘hameçonnage. En règle générale, un protocole d‘authentification par défi/réponse comme le suivant est mis en œuvre :

- Le serveur envoie un défi au client. Le défi comprend un nombre aléatoire, l‘heure actuelle et l‘URL du serveur.
- Le client signe la demande et la renvoie au serveur en tant que réponse.
- Le serveur vérifie la signature. Si elle est correcte et si le défi est inchangé, l‘authentification est réussie.

Authentification basée sur certificat électronique

L‘authentification basée sur la signature exige que le serveur connaisse la clé de signature publique du client. Bien sûr, le client peut y parvenir en envoyant sa clé de signature publique avec la réponse, mais dans ce cas, la clé publique peut ne pas être authentique. La façon la plus évidente d‘établir l‘authenticité de la clé est d‘utiliser des certificats numériques. Dans ce cas, le protocole d‘authentification fonctionne comme suit:

1. Le serveur envoie un défi (comprenant un nombre aléatoire, l‘heure actuelle et l‘URL du serveur) au serveur.
2. Le client signe le défi et le renvoie au serveur en tant que réponse. En outre, il envoie son certificat numérique, qui comprend sa clé publique.
3. Le serveur vérifie la signature et le certificat numérique. Si tout est correct, l‘authentification est réussie.

L‘authentification par certificat résiste à l‘hameçonnage car la réponse comprend l‘URL signée du serveur. En cas d‘attaque par hameçonnage, l‘URL du serveur attaquant est signée.

Dans le cas d‘une attaque par hameçonnage, l‘URL du serveur attaquant est signée. Si l‘attaquant ne modifie pas cette URL, le serveur n‘acceptera pas la réponse, car elle contient une URL erronée. Si l‘attaquant modifie l‘URL, le serveur n‘acceptera pas la réponse car la signature est erronée.

Pour améliorer la sécurité, la technique du token binding peut être utilisée[22]. Cela signifie que le client signe non seulement un défi, mais aussi un ensemble de données (token) qui contient son identité et éventuellement d‘autres informations telles qu‘une URL. Un jeton peut être utilisé au cours de plusieurs sessions de protocole. Pour un attaquant, il est pratiquement impossible de falsifier un jeton et il est inutile d‘en voler un, car les informations d‘identité contenues se réfèrent à une instance différente et ne peuvent pas être modifiées.

Public Key Infrastructure (PKI)

L‘authentification par certificat nécessite l‘existence d‘une infrastructure permettant l‘émission et la distribution de certificats numériques. En d‘autres termes, une infrastructure à clé publique (PKI en anglais)) est nécessaire. Dans de nombreux cas, une PKI d‘entreprise existante peut être utilisée. Si ce n‘est pas le cas, on peut faire appel à une autorité de certification (AC) publique ou à une offre de PKI en tant que service. Il est également possible de créer une nouvelle PKI et de l‘utiliser pour l‘authentification par certificat ainsi que pour d‘autres applications.

La PKI représente une technologie de sécurité éprouvée qui protège contre de nombreuses attaques différentes. Cette approche s’avère efficace depuis plus de 25 ans. L‘utilisation d‘une PKI pour l‘authentification par certificat est une méthode répandue et fiable. L‘application de cette technologie dans le domaine de la résilience au phishing est donc une étape logique qui repose sur des mécanismes bien compris. L‘utilisation de signatures numériques qualifiées et le chiffrement des courriels peuvent encore améliorer la protection contre l’hameçonnage fournie par une PKI.

L‘authentification FIDO

Au lieu d‘une PKI, l‘infrastructure d‘authentification FIDO peut être utilisée pour authentifier la clé de signature publique du client. FIDO, qui signifie „Fast Identity Online“, est une association industrielle ouverte et un ensemble de normes et de protocols conçus pour améliorer l‘authentification en ligne. FIDO Alliance, l‘organisation à l‘origine de FIDO, a été créée pour répondre aux défis croissants associés aux méthodes d‘authentification traditionnelles basées sur des mots de passe, qui sont souvent vulnérables à diverses formes de cyber-attaques, y compris le phishing.

Fonctionnement FIDO

Les méthodes d‘authentification FIDO permettent à chaque utilisateur de générer sa propre paire de clés pour chaque serveur qu‘il utilise. Sur la base de cette paire de clés, l‘authentification basée sur la signature est appliquée, comme indiqué ci-dessus. Bien que moins sûre que les certificats numériques, la méthode FIDO est plus facile à utiliser dans les environnements qui ne comprennent pas de PKI. Toutefois, contrairement à une PKI, l‘utilisation de l‘authentification FIDO ne peut pas être étendue aux signatures numériques, au chiffrement et à divers autres cas d‘utilisation de l‘authentification, y compris l‘accès VPN.

Une fois encore, la raison pour laquelle ce système résiste à l‘hameçonnage est que l‘URL du serveur fait partie du message signé. La liaison avec un Token, qui renforce encore la sécurité, peut également être utilisée.

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

L’infrastructure FIDO

L‘authentification FIDO est une technologie mature qui est utilisée dans différents contextes à travers le paysage numérique, y compris les services en ligne, les sites web, les services financiers, l‘authentification d‘entreprise, les services gouvernementaux, les soins de santé, les services cloud, l‘éducation, les appareils IoT, les applications mobiles et l‘authentification multiplateforme.

L‘adoption de l‘authentification FIDO continue de croître à mesure que les organisations reconnaissent ses avantages en termes de sécurité, d‘expérience utilisateur et de protection de la vie privée. Les utilisateurs peuvent tirer parti des appareils et des méthodes d‘authentification compatibles avec FIDO pour améliorer la sécurité de leurs comptes et de leurs transactions en ligne.

La protection des messages de bout en bout

Rendre le processus d‘authentification plus sûr grâce aux signatures numériques n‘est pas la seule approche pour se protéger du phishing. Il est également utile de prévenir les courriels d‘hameçonnage.

La protection cryptographique de bout en bout

Pour protéger un courrier électronique d‘une lecture non autorisée, il est conseillé d‘utiliser le chiffrement. Le chiffrement moderne est basé sur la cryptographie asymétrique avec des algorithmes tels que RSA et Diffie-Hellman. Si, en plus, une protection contre la falsification des courriels est nécessaire, il convient d‘utiliser des signatures numériques. Les signatures numériques sont également basées sur la cryptographie asymétrique. Le chiffrement et les signatures numériques sont des techniques similaires qui peuvent facilement être déployées et utilisées ensemble.

Pour sécuriser efficacement les courriels au moyen de la cryptographie, l‘approche recommandée consiste à utiliser le chiffrement et les signatures de bout en bout. Cela implique d‘effectuer le chiffrement, la signature, le déchiffrement et la vérification directement sur l‘ordinateur de l‘utilisateur.

La protection cryptographique du courrier électronique dans une entreprise devrait être utilisée avec l‘appui d‘une PKI. Bien qu‘il soit également possible d‘utiliser une distribution de clés hors bande, cela n‘est conseillé que pour un petit groupe d‘utilisateurs. Bien entendu, la même PKI peut être utilisée pour la protection du courrier électronique et l‘authentification basée sur des certificats. Les certificats peuvent être fournis par une PKI interne ou un service tiers proposé, par exemple, par une autorité de certification publique ou une offre de PKI en tant que service, qui peut être hébergée dans le Cloud.

Comment les signatures et le chiffrement de courriels protègent du phishing

Les signatures numériques offrent une bonne protection contre les courriels d‘hameçonnage. Si les courriels légitimes sont systématiquement signés, l‘utilisateur comprendra immédiatement qu‘un courriel non signé est suspect.

Le chiffrement des courriels est également utile pour résister au phishing, car un attaquant doit utiliser la clé publique du destinataire pour falsifier un courriel crédible. Bien que cela soit possible, la préparation d‘un courriel d‘hameçonnage nécessite une étape supplémentaire, ce qui rend l‘hameçonnage plus difficile. En outre, l‘envoi de courriers identiques à des milliers de destinataires ne fonctionne pas dans ce cas.

Dans l‘ensemble, la signature et le chiffrement augmentent la sécurité du courrier électronique de nombreuses façons. La protection contre l‘hameçonnage n‘est qu‘un des nombreux avantages qu‘offre cette technologie.

Deploiement

Le déploiement d‘une protection cryptographique du courrier électronique est un projet d‘intégration de systèmes. Pour la gestion des certificats numériques, il est souvent possible d‘utiliser une PKI existante. En outre, de nombreux fournisseurs proposent des services de PKI, y compris des solutions basées sur le Cloud et des solutions de PKI en tant que service. Le chiffrement et la signature des courriels sont utilisés par de nombreuses organisations dans le monde entier depuis plus de 20 ans. Il s‘agit d‘une technologie bien établie, dont la portée va bien au-delà de la prévention de l‘hameçonnage. Dans un avenir proche, les PKI devront être équipées d‘algorithmes de cryptographie post-quantique pour les rendre résistantes aux attaques des ordinateurs quantiques.

Les solution Eviden Digital Identity

Eviden regroupe ses lignes d'activités numériques, cloud et big data & security. Il s'agit d'un leader mondial de la transformation numérique axée sur les données, transparente et durable. Entreprise numérique de nouvelle génération, Eviden s'appuie sur des positions de leader mondial dans les domaines du numérique, du cloud, des données, de l'informatique avancée et de la sécurité.

Eviden Digital Identity rassemble les solutions cryptovision, CardOS et IDnomic, développées pour protéger les identités électroniques à l'aide de solutions et d'applications cryptographiques.

Eviden Digital Identity fournit plusieurs solutions puissantes qui empêchent les attaques de phishing. En outre, le portefeuille d'Eviden comprend des produits qui mettent en œuvre des mots de passe à usage unique, notamment CardOS SmartOTP et HOTP/TOTP. Cependant, ces solutions ne sont pas pertinentes pour la résilience au phishing.

Figure 5: Le système d'exploitation des cartes à puce CardOS prend en charge à la fois l'authentification FIDO et l'authentification par certificat.

L'offre Eviden pour l'authentification par certificat

Eviden Digital Identity fournit un portefeuille de solutions qui permettent l'utilisation de l'authentification basée sur des certificats :

- **CardOS** : ce système d'exploitation pour cartes à puce prend en charge à la fois l'authentification FIDO et l'authentification par certificat.
- **cryptovision ePasslet Suite** : La cryptovision ePasslet Suite est un ensemble basé sur Java Card pour les cartes à puce, qui prend en charge l'authentification par jeton FIDO et par certificat.
- **cryptovision SCinterface** : Cette solution représente un logiciel indépendant de la plate-forme pour l'utilisation de cartes à puce et de jetons. Elle comprend des extensions optionnelles pour la convivialité et la satisfaction de l'utilisateur, notamment VirtualSmartCard et RemoteSmartCard. Elle prend en charge l'authentification par certificat, les signatures numériques et le chiffrement.
- **IDnomic PKI** : IDnomic PKI est une solution robuste et puissante d'autorité de certification mutualisée. Elle peut être utilisée, entre autres, pour opérer une PKI pour l'authentification basée sur des certificats et la protection du courrier électronique.
- **IDnomic CMS** : Le Credential Management System (CMS) d'IDnomic améliore la gestion des certificats numériques dans une PKI et facilite l'administration globale des supports cryptographiques. Parmi les applications PKI prises en charge figurent l'authentification par certificat et la protection du courrier électronique.
- **IDnomic CLM** : Cette solution de gestion du cycle de vie des certificats (CLM) prend en charge un certain nombre de fonctions utiles qui facilitent l'utilisation d'une PKI, en particulier dans les environnements hétérogènes. L'authentification basée sur des certificats et la protection du courrier électronique peuvent en bénéficier.
- **IDnomic Sign** : IDnomic Sign permet des signatures numériques sécurisées qui peuvent être utilisées, entre autres, pour la protection contre le phishing.
- **Evidian Web Access Manager** : Le gestionnaire d'accès Web d'Evidian comprend un reverse-proxy qui permet une authentification centralisée. Il offre une gamme de méthodes d'authentification forte, y compris l'authentification par certificat et FIDO avec liaison de jeton. Une fois authentifiés, les utilisateurs n'ont accès qu'aux ressources pour lesquelles ils disposent des permissions appropriées, ce qui permet de se prémunir contre les tentatives d'hameçonnage et les accès non autorisés.

L’offre Eviden pour l’authentification FIDO

Les produits Eviden suivants supportent l‘authentification FIDO :

- **CardOS** : Le système d‘exploitation pour cartes à puce CardOS prend en charge à la fois l‘authentification par jeton FIDO et l‘authentification par certificat (cette dernière est obtenue par l‘utilisation de l‘applet ePKI de SCinterface). Deux facteurs de forme sont disponibles : un jeton avec interface USB et NFC ainsi qu‘une carte à puce traditionnelle avec interface avec ou sans contact. CardOS FIDO2 est une application certifiée FIDO pour les cartes à puce CardOS, permettant de les utiliser comme authentificateur FIDO.
- **Evidian Web Access Manager** : Evidian Web Access Manager supporte une gamme de méthodes d‘authentification forte, y compris l‘authentification par certificat et FIDO avec liaison de jeton.

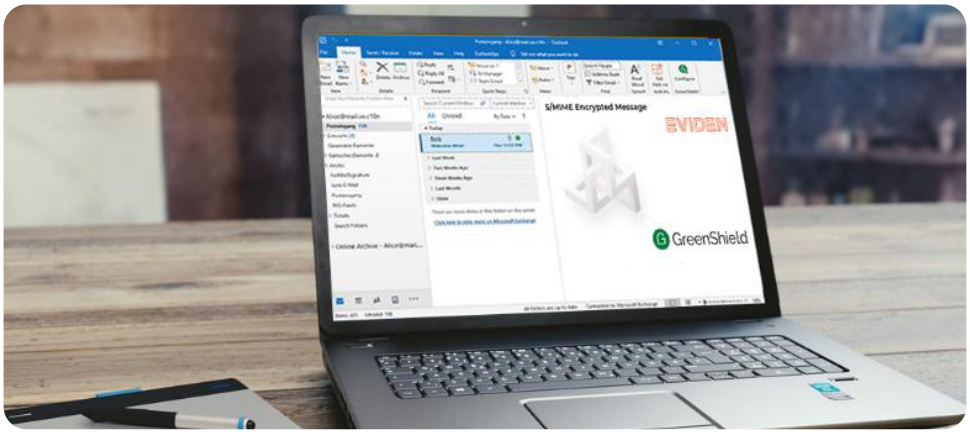


Figure 6: cryptovision GreenShield offre une protection de bout en bout des courriels et des fichiers, intégrée à Outlook et à Notes.

L’offre Eviden pour la protection cryptographique de courriels

Eviden fournit plusieurs outils performants pour la protection des courriels :

- **Cryptovision GreenShield**: fournit un système de chiffrement/signature de bout en bout des courriels et des fichiers, intégré de manière transparente dans Microsoft Outlook et HCL (Lotus) Notes. Cryptovision GreenShield est approuvé pour les informations classées VS-NfD, OTAN, UE.
- **Cryptovision GreenShield Comfort**: Il s‘agit d‘une solution complète fournissant un chiffrement de bout en bout, des services PKI ainsi que la gestion du cycle de vie des clés et des certificats, contrôlée par des processus automatisés.

La résistance à l‘hameçonnage n‘est qu‘un des nombreux objectifs qui peuvent être atteints grâce à ces solutions.

Les références d’Eviden

Eviden Digital Identity possède deux décennies d‘expérience en matière d‘authentification basée sur des certificats, de PKI et de cryptage de bout en bout des courriels. La liste suivante mentionne quelques clients :

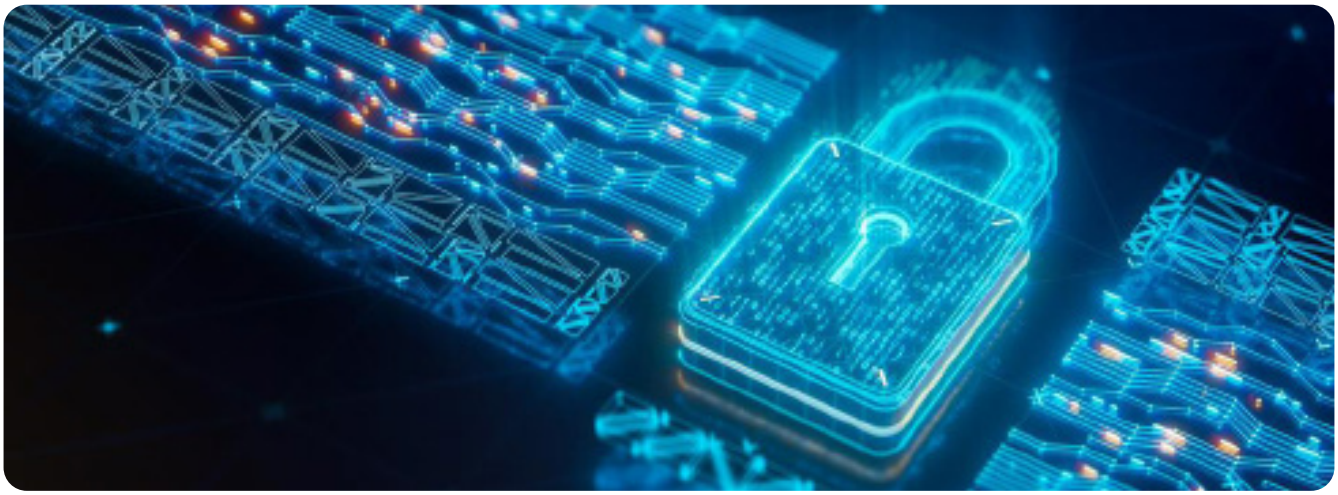
- ADAC: Authentification par certificat
- Airbus: Solution PKI
- Allianz: Authentification par certificat, signature & PKI
- BNP Paribas: Solution PKI
- Bouygues Telecom: Solution PKI
- Bundesministerium für Finanzen: Email sécurisée & Solution PKI
- Bundesministerium für Bildung und Forschung: Email sécurisée & Solution PKI
- Bundeswehr: Sécurité d’email avec cryptovision GreenShield Mail
- City of New York: Solutions PKI
- Credit Agricole: Solution PKI
- Deutsche Telekom: Solution de chiffrement de données et de fichiers
- e.on: Authentification par certificat & solution de signature
- EDF: Solution PKI
- European Commission: IDnomic PKI pour C-ITS (systems de transport intelligents)
- European Patent Office: Authentification par certificat & solution de signature
- Ministère de la Santé et de la Prévention: Solution PKI
- Ministère de l’Éducation nationale: Solution PKI
- Postbank: Solution PKI
- SAP: Solution d’email sécurisé

Pourquoi il est essentiel d'investir dans des technologies résistantes au Phishing ?

Les attaques par hameçonnage servent souvent de point d'entrée aux acteurs malveillants pour compromettre le réseau d'une organisation. Investir dans des technologies résistantes au phishing permet donc de protéger les actifs numériques et la propriété intellectuelle d'une entreprise.

Être victime d'une attaque de phishing n'expose pas seulement une organisation à des risques financiers et opérationnels immédiats, mais ternit également sa réputation. Lorsque les données des clients sont compromises ou que les services sont interrompus, la confiance est érodée et les clients peuvent chercher d'autres solutions.

Le paysage réglementaire entourant la protection des données et la cybersécurité est en constante évolution. De nombreuses lois et réglementations relatives à la protection des données, telles que le GDPR, l'HIPAA et le CCPA, imposent aux organisations des exigences strictes en matière de protection des informations sensibles contre l'accès ou la divulgation non autorisés. Le non-respect de ces réglementations peut entraîner de lourdes pénalités financières et des conséquences juridiques. Investir dans des technologies résistantes au phishing permet non seulement de se mettre en conformité en empêchant l'accès non autorisé à des données sensibles, mais aussi de montrer l'engagement d'une organisation à respecter ses obligations légales. Cette attitude proactive peut contribuer à éviter des procédures juridiques coûteuses et des amendes réglementaires.



Conclusion

En conclusion, les attaques de phishing représentent un danger évident et actuel pour les organisations de toutes tailles et de tous secteurs. En investissant dans des technologies de pointe résistantes au phishing, les entreprises peuvent réduire considérablement les risques, protéger leurs actifs, maintenir une réputation impeccable, inspirer la confiance des clients et remplir leurs obligations légales. Dans la lutte actuelle contre les cybermenaces, ces technologies jouent un rôle crucial dans le renforcement des défenses numériques des entreprises contemporaines, garantissant ainsi un avenir sûr, robuste et conforme.

Eviden Digital Identity propose une gamme convaincante de produits et de stratégies que les organisations peuvent utiliser pour améliorer leur résilience face à la menace omniprésente des attaques de phishing. Pour en savoir plus sur notre offre, veuillez nous contacter ici :
cv-info@eviden.com
www.cryptovision.com
Notre équipe de consultants sera heureuse de vous contacter.

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

A propos d'Eviden[1]

Eviden est un leader technologique de la prochaine génération dans la transformation numérique axée sur les données, fiable et durable, avec un solide portefeuille de technologies brevetées. Avec des positions de leader mondial dans les domaines de l'informatique avancée, de la sécurité, de l'IA, du cloud et des plateformes numériques, elle offre une expertise approfondie pour tous les secteurs dans plus de 47 pays. Réunissant 53 000 talents de classe mondiale, Eviden élargit les possibilités des données et de la technologie à travers le continuum numérique, aujourd'hui et pour les générations à venir. Eviden est une société du groupe Atos qui réalise un chiffre d'affaires annuel d'environ 5 milliards d'euros.

[1] Les activités d'Eviden sont exploitées par le biais des marques suivantes : 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 est une marque déposée. © Eviden SAS, 2023.

A propos Atos

Atos est un leader mondial de la transformation numérique avec 105 000 employés et un chiffre d'affaires annuel d'environ 11 milliards d'euros. Numéro un européen de la cybersécurité, du cloud et de l'informatique haute performance, le Groupe fournit des solutions de bout en bout sur mesure pour tous les secteurs d'activité dans 69 pays. Pionnier dans les services et produits de décarbonisation, Atos s'engage pour un numérique sécurisé et décarbonisé pour ses clients. Atos est une SE (Societas Europaea) cotée sur Euronext Paris.

L'objectif d'Atos est d'aider à concevoir l'avenir de l'espace d'information. Son expertise et ses services soutiennent le développement de la connaissance, de l'éducation et de la recherche dans une approche multiculturelle et contribuent au développement de l'excellence scientifique et technologique. Partout dans le monde, le Groupe permet à ses clients, à ses employés et aux membres de la société dans son ensemble de vivre, de travailler et de se développer de manière durable, dans un espace d'information sûr et sécurisé.

Connectez-vous

eviden.com

 20240119