wallix

03

L'accès légitime, angle mort de la cybersécurité bancaire



wallix

En 2026, inutile de braquer le guichet pour dévaliser la banque.

Il suffit de passer par le cyberespace, et, derrière leurs écrans, les acteurs de la cybercriminalité l'ont bien compris. Cela peut même se faire de manière très discrète, en ouvrant une session valide, avec un compte lui aussi valide, puis en contournant et relayant l'authentification forte.

Selon un rapport de Citalid publié en septembre, les attaquants cherchent de plus en plus à agir sous l'apparence d'un utilisateur ou d'un collaborateur légitime, sans pour autant supprimer les opérations d'exploitations de vulnérabilités ou d'autres vecteurs d'attaques plus traditionnels.

wallix

Dans ce contexte, l'identité, la session et l'accès légitime deviennent des surfaces d'attaque convergentes.

Pourtant, le secteur bancaire est l'un des plus matures en cybersécurité, grâce à la numérisation massive de ses activités, à sa capacité à innover et à des textes législatifs adaptés aux nouvelles menaces.

C'est précisément pour cette raison que les attaquants évitent de plus en plus la confrontation directe pour viser les angles morts de la confiance. Comment empêcher que les accès légitimes ne deviennent le talon d'Achille de la cybersécurité bancaire ?

wallix

L'essentiel :

1

L'identité est devenue la cible principale.

Avec le MFA généralisé, les attaquants visent ce qui se passe avant, pendant, après et autour de l'authentification. Un compte légitime compromis échappe aux outils de détection classiques.

2

La confiance doit être vérifiée en continu.

Il ne suffit plus de savoir « qui êtes-vous ? », il faut aussi surveiller « que faites-vous ? ». Cela vaut pour toutes les identités, y compris les prestataires et les agents IA.

3

Le PAM limite l'impact d'une usurpation.

Inventaire des privilèges, accès just-in-time, MFA résistant au phishing et surveillance des sessions garantissent qu'une identité volée ne suffit pas à tout compromettre.

Pourquoi l'identité est devenue la cible privilégiée des attaquants ?

En 2026, la plupart des acteurs du secteur bancaire ont conscience de l'importance d'implémenter un MFA au sein de leur organisation, afin de protéger les accès au système d'information.

Par exemple, les évaluations CBEST de la Bank of England publiées en 2026 ne présentent plus la mise en place d'un MFA comme un manquement, contrairement aux publications de 2023 et 2024.

Cela a contribué à déplacer la menace : les attaquants ne cherchent plus à voler un mot de passe, ils ciblent ce qui se passe après l'authentification (session) ou autour d'elle (procédures de récupération ou de support).



L’identité concentre la valeur dans un système d’information bancaire, c’est pour cela qu’elle intéresse les attaquants.

Elle peut donner accès aux flux de paiement, aux données clients et aux outils de conformité, qui sont autant d’éléments critiques pour les établissements bancaires. Un compte valide compromis hérite des privilèges et de la légitimité qui lui sont associés. Cela réduit fortement la probabilité que l’intrusion ne soit détectée.

wallix

Pourquoi l'identité est devenue la cible privilégiée des attaquants ?

Avec la numérisation massive du secteur bancaire, il faut désormais gérer des identités humaines (collaborateurs internes, prestataires), mais aussi non humaines (comptes de service, API, applications SaaS connectées par Oauth… Et bientôt, les agents IA s'ajouteront à cela !).

La surface d'attaque s'est donc démultipliée. Le cloud et le SaaS ont fait de l'identité le véritable périmètre à sécuriser : le réseau ne joue plus ce rôle.

Enfin, on observe que de plus en plus d'acteurs cybercriminels, même les moins qualifiés, ont accès à la sophistication.

wallix

Les offres de Phishing-as-a-Service (PhaaS) et de Malware-as-a-Service (MaaS) démocratisent les chaînes d'attaque complexes, à la portée de n'importe quel opérateur, moyennant finance.

Par exemple, au printemps 2026, les équipes de Varonis et de Netcraft ont découvert BlueKit, un kit payant qui met à disposition des acheteurs des éléments permettant des attaques très sophistiquées visant l'identité, dont certaines concernent des banques et des plateformes de cryptomonnaies.

wallix

L'identité peut-elle être attaquée avant le processus d'authentification ?

L'identité peut être la cible d'attaque avant, pendant, après et autour de l'authentification. Cela demande donc une vigilance de tout instant la concernant.

Avant l'authentification, l'attaquant a plusieurs moyens d'obtenir des accès à la banque qui l'intéresse.

L'un des plus simples consiste à acheter des identifiants, via des marchés d'infostealers ou grâce à des courtiers en accès initial sur le darknet. C'est un moment où l'attaquant peut également faire preuve de finesse et exploiter les failles humaines grâce à des techniques d'ingénierie sociale.

wallix

L'identité peut-elle être attaquée avant le processus d'authentification ?

C'est ce qui est par exemple arrivé au Brésil de fin juin à début juillet 2025 : les attaquants ont approché et recruté un jeune opérateur de l'entreprise C&M Software (qui fournit services intermédiaires reliant les fintechs et banques au système de paiement instantané PIX).

Celui-ci a été convaincu et leur a vendu ses identifiants professionnels pour une somme dérisoire. Grâce à cela, les commanditaires ont donc pu infiltrer 6 institutions bancaires et dérober 100 millions de dollars.

Plus récemment, on a aussi eu un exemple d'infiltration sous fausse identité avec les faux travailleurs informatiques nord-coréens aux Etats-Unis.



Dans ce cas, c'est l'organisation elle-même qui leur a accordé des équipements et des droits d'accès.

Par souci de confidentialité, le nom des institutions bancaires n'a pas été communiqué par les enquêteurs.

Les attaquants peuvent-ils relayer ou détourner l'authentification ?

Les attaquants peuvent aussi relayer ou détourner l'authentification, pour obtenir les accès pendant le processus.

Il existe une technique d'attaque qui s'appelle « Proxy Adversary in the Middle » , celle-ci consiste à relayer en temps réel les échanges et à capturer les identifiants et les jetons de sessions. Ainsi, il est possible de contourner les MFA classiques (OTP, push).

Ils peuvent aussi recourir à une autre technique : intercepter les l'OTP via les SMS ou un maliciel mobile qui abuse des services d'accessibilité Android.

wallix

Par exemple, il existe un compte de piratage clé en main appelé EvilTokens, qui contient une attaque « Device Code » .

Celle-ci consiste à piéger une victime en lui faisant valider un code sur la vraie page officielle de Microsoft.

L'attaquant récupère ainsi directement les jetons d'accès à son compte Microsoft 365, contournant totalement le mot de passe et le double facteur (MFA) sans avoir besoin de créer un faux site web.

L’identité peut-elle être la cible d’attaques après l’authentification ?

Après l’authentification, l’identité est encore susceptible d’être attaquée.

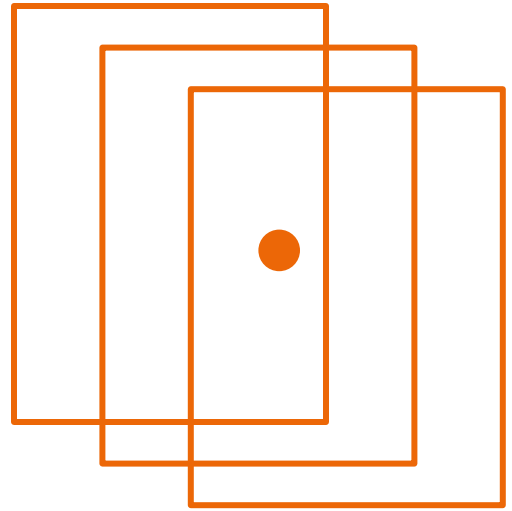
L’attaquant peut rejouer une session grâce à des vols de cookies ou de jetons, alors que celle-ci avait déjà été validée par MFA.

Les cybercriminels peuvent aussi effectuer la fraude directement sur le smartphone de la victime (on-device fraud), lorsque celle-ci est connectée ou via des services d’accessibilité préautorisés.

Pour détecter ce type de manœuvre, les banques ont mis en place des moteurs de biométrie comportementale, capables d’identifier les scripts automatiques.

wallix

Cependant, les cybercriminels s'adaptent toujours aux obstacles posés par les professionnels de la cybersécurité : il existe un outil qu'ils peuvent se procurer, Herodotus, qui permet d'imiter le rythme humain.

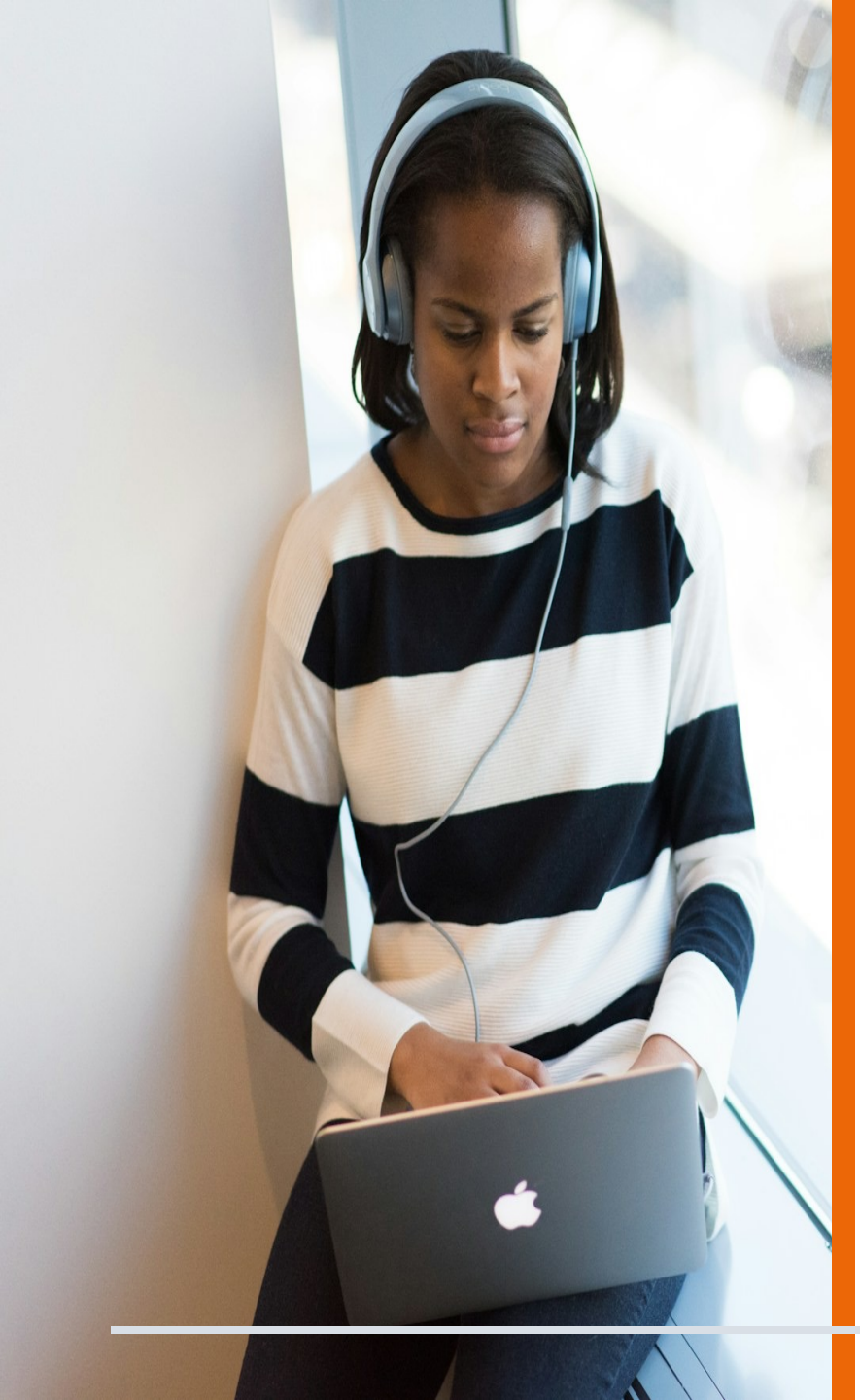


wallix

Les attaquants peuvent-ils mener des actions en périphérie de l'authentification pour récupérer des indentifiants ou des mots de passe ?

L'identité peut-être également la cible des cyberattaquant, via des actions périphériques à l'authentification auxquelles on prête parfois moins attention. Ainsi, les procédures de récupération d'identifiants ou de mots de passe via le helpdesk peuvent attiser les intentions malveillantes.

En effet, un simple appel peut suffire pour obtenir une réinitialisation de mot de passe ou de facteur MFA quand on a la bonne information. Et celle-ci peut être simple à obtenir si on a recours à la bonne technique d'ingénierie sociale.



Ceci est facilité par le fait que les agents vocaux peuvent être utilisé dans ces campagnes, que ce soit du côté du support ou de celui des attaquants.

Les centres d'aide et les helpdesk ne sont donc plus aujourd'hui qu'une fonction support, ils participent aussi à l'administration et à la sécurisation de l'identité numérique.

Qu'est-ce que l'évolution de cette menace change pour les banques ?

Cette tendance de la menace implique quelques changements pour les établissements bancaires afin de maintenir une cybersécurité efficace.

Tout d'abord, cela remet en cause tout ce qui avait été mis en place pour lutter contre les intrusions. En ciblant l'identité, l'attaquant se comporte comme un « insider » et les outils qui avait été mis en place pour le détecter (EDR, IDS) ne détectent pas d'activité anormale.

Face à l'évolution de la menace, une chose est certaine : l'authentification initiale ne suffit plus comme point de contrôle.

wallix

La confiance doit être réévaluée en continu, via la supervision comportementale, le contrôle des applications connectés, la vérification indépendante des opérations sensibles, la recherche d'incohérences après l'attribution des droits.

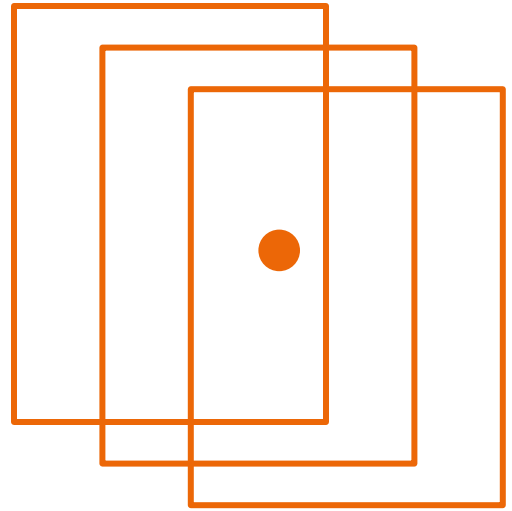
Un tel niveau de vigilance est crucial pour le secteur bancaire.

Il est nécessaire d'être tout aussi vigilant avec les tiers et les prestataires.

Ces accès distants sont devenus une véritable opportunité pour les attaquants, car ils comptent parmi ceux qui ont les privilèges les plus élevés tout en étant paradoxalement les moins surveillés.

wallix

Le cas de C&M Software que l'on a évoqué précédemment illustre bien cet enjeu : pour compromettre des institutions bancaires au Brésil, l'attaquant a ciblé un intermédiaire disposant d'un accès à privilèges sur une infrastructure de paiement.



wallix

Qu'est-ce que l'évolution de cette menace change pour les banques ?

L'enjeu de cette évolution de la menace est aussi économique.

La compromission d'un compte à privilèges peut avoir des conséquences à la fois désastreuses et onéreuses : exfiltration de données, extorsion, prépositionnement… L'identité et les accès légitimes sont une mine d'or pour les groupes cybercriminels.

Les régulateurs l'ont bien compris, et on observe depuis quelques années un renforcement réglementaire à ce sujet.



wallix

Par exemple, le règlement européen DORA, applicable depuis janvier 2025, impose des exigences qui relèvent de la gestion des identités et des accès, de la maîtrise des prestataires tiers et de la notification des incidents majeurs, avec des sanctions à la clé pour ceux qui ne les respecteraient pas.

Côté BCE, la résilience cyber figure parmi les axes d'inspection sur site, selon les priorités de supervision 2026-2028.

En parallèle, le SWIFT CSCF et le PCI DSS v4.0 exigent également des mesures explicites concernant les comptes à privilèges et le MFA.



Les établissements bancaires ont donc tout intérêt à développer leur gestion des identités et des accès, ne serait-ce qu'en considérant cela comme un levier de conformité.

wallix

Comment garantir qu'une identité usurpée ne compromettra pas le système ?

Puisqu'il est devenu impossible de garantir qu'aucune identité ne sera usurpée, il faut garantir qu'une identité usurpée ne suffira jamais à tout compromettre. Telle est la promesse du Privileged Access Management (PAM).

Cette discipline de la cybersécurité, rattachée à l'IAM (gestion des identités et des accès) apporte une solution concrète pour mieux contrôler les privilèges existants. Rappelons le CBEST, un des cadres de tests de cybersécurité pour le secteur bancaire parmi les plus exigeants d'Europe, relève encore aujourd'hui des comptes administrateurs et de services trop permissifs.



Souvent, cette négligence ne relève pas de mauvaises intentions mais tout simplement parce que l'on oublie le niveau de privilèges précédemment accordé.

La première étape pour implémenter le PAM dans son établissement bancaire consiste à réaliser un inventaire de tous les accès à privilèges existants, afin d'avoir une véritable perspective sur la situation de départ.

Cet inventaire pose les fondations pour appliquer les autres principes du PAM, comme la mise en place d'un coffre-fort et de la rotation des secrets, puis l'attribution d'accès just-in-time lorsque cela est nécessaire.

wallix

Ces quelques mesures rendent déjà le jeton volé ou la session compromise bien moins intéressants pour l'attaquant, puisque le privilège n'existe que pour quelques minutes.

wallix

Comment garantir qu'une identité usurpée ne compromettra pas le système ?

Il est recommandé aux établissements bancaires de mettre en place des MFA résistants au phishing pour tout action liée à des accès à privilèges. C'est aussi une mesure qui fait partie des principes du PAM, couplée à un autre élément : l'enregistrement des sessions.

En effet, être authentifié ne signifie pas pour autant être digne de confiance. Pour cela, il est possible d'enregistrer et de surveiller les sessions, avec une coupure en temps réel si l'activité est jugée suspecte.

wallix

Cela change la donne, car l'attaquant peut être bloqué avant même de créer des dégâts, dont les conséquences pourraient être vraiment dommageables pour les institutions bancaires.

Le PAM propose une vision complète sur les accès des établissements, puisqu'il repose sur le fait que le privilège ne se limite pas aux administrateurs. Dans cette logique, il prend également en compte les accès des prestataires, du helpdesk, des comptes techniques et même des agents IA.

Ceux-ci peuvent tout autant être la cible des attaquants que les administrateurs, c'est pourquoi il est nécessaire de maîtriser leur niveau de privilèges.

wallix

Désormais, les établissements bancaires ne doivent plus se contenter de pouvoir répondre à la question « qui êtes-vous ? ».

Une gestion efficace des accès et des identités impose de pouvoir également répondre aux questions « que faites-vous ? » et « pourquoi maintenant ? » afin d'anticiper une menace toujours plus discrète. Au-delà de l'authentification, il s'agit désormais de gouverner la confiance tout au long de la session et du cycle de vie.

wallix

Le secteur bancaire gagnera à développer cette vigilance sur le long terme au vu de l'évolution de la menace : demain, les attaquants pourraient aller plus loin que le simple vol d'accès, mais pourraient également chercher à faire valider une décision par une identité légitime, qu'elle soit humaine ou un agent IA.

Dans l'immédiat, réduire le nombre de privilèges permanents est probablement le levier au meilleur rapport coût-efficacité pour faire face à cette menace.