ALSID ACADEMY

Episode 7

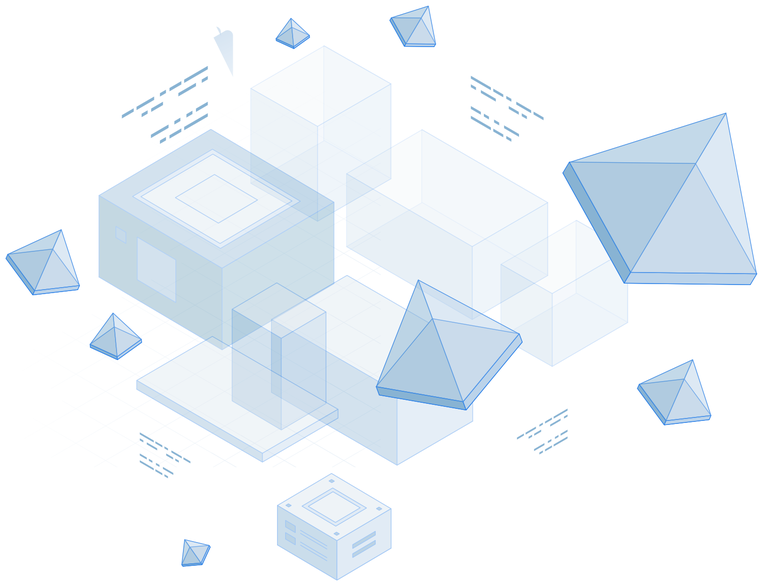
HACKERS VS BANQUE & FINANCE : LES BONS COMPTES DU RSSI

Depuis quelques années, les institutions financières et bancaires du monde entier sont les victimes favorites de nombreux groupes cybercriminels. Leurs attaques, ciblées, permettent de détourner des quantités d'argent croissantes et impactent la stabilité de production et la réputation des organisations visées.

Il apparait évident que les responsables IT ainsi que les responsables sécurité de ces institutions doivent investir du temps afin d'étudier et comprendre les cybermenaces particulières qui les touchent et ainsi mettre en œuvre les contremesures nécessaires à la sauvegarde de l'activité bancaire ou financière.

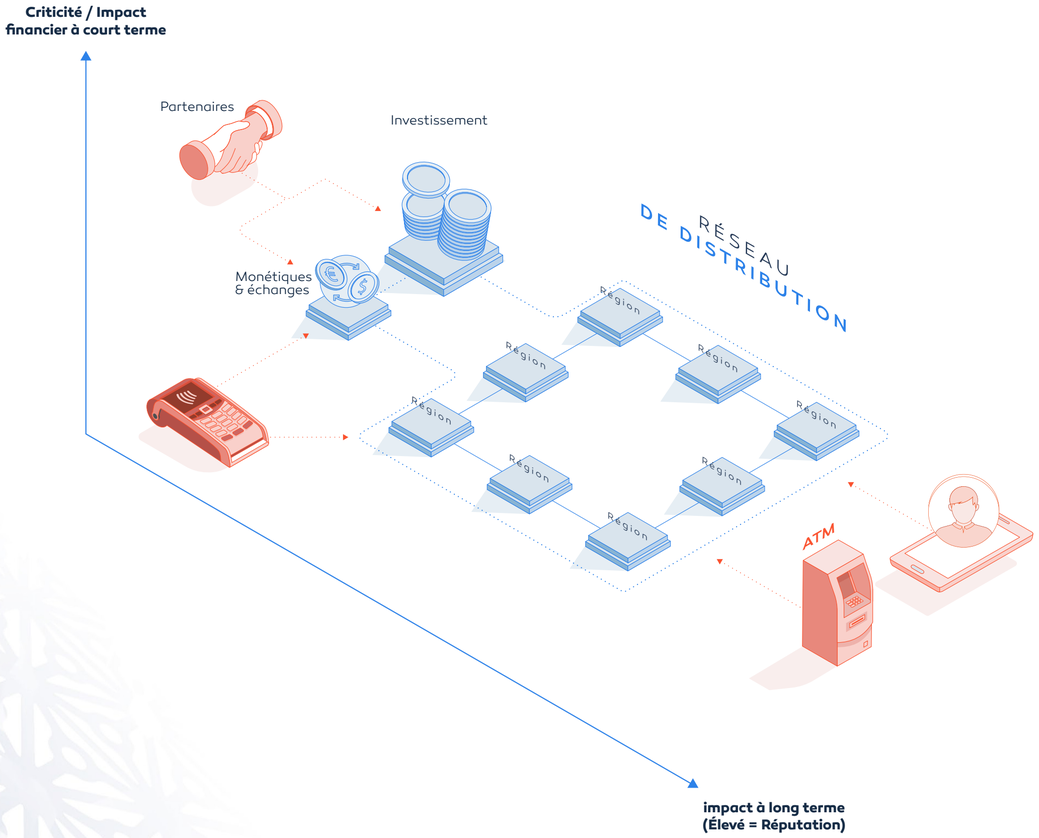
DE LA PARTICULARITÉ DES SYSTÈMES D'INFORMATION BANCAIRES OU FINANCIERS

Les systèmes d'information bancaires et financiers possèdent des particularités qui tendent à rendre leur protection plus complexe que des environnements IT traditionnels.



- Multiplicité des systèmes d'information : les systèmes d'informations (SI) bancaires sont par essence éclatés en plusieurs sous-SI rattachés les uns aux autres, rendant extrêmement complexe la cohérence de bout en bout. Cette complexité, ce morcellement, qu'il soit voulu ou subi, induit irrémédiablement des faiblesses structurelles
- Ouverture du SI vers l'extérieur : les systèmes bancaires ou d'assurances doivent être ouverts vers l'extérieur : premièrement aux client usagers désirant accéder à leur interface de gestion, deuxièmement aux tiers de confiance et partenaires d'intermédiation, afin d'assurer les mouvements financiers ou fiduciaires. Les SI sont interconnectés à différentes entités extérieures que l'on peut nommer au sens large du terme « partenaires »
- Il s'agit d'une cible particulièrement attractive pour les attaquants : vcomplexité et le temps d'incubation de l'attaque) mais aussi les SI portant les plus belles promesses de rentabilité. Sur ce dernier point, un système bancaire ou financier représente cible particulièrement alléchante

Nous pouvons simplifier la représentation des systèmes bancaires ou financiers selon le schéma suivant :



Les trois SI principaux constitutifs des institutions financières possèdent généralement les caractéristiques suivantes :

- **SI du Réseau de distribution :** que ce soit dans le monde bancaire ou assurance, ce SI est par nature connecté aux usagers et aux différents automates nécessaires à l'activité. De plus ce SI est très souvent composé de l'association de plusieurs SI régionaux, qui historiquement composaient des SI autonomes. Du fait de sa visibilité, la compromission de ce SI peut générer un impact fort sur la réputation de l'établissement

  SI Monétique & Echanges : ce SI gère l'interaction avec les tiers de confiance, historiquement ce SI est centralisé par le groupe et est soumis aux contrôles PCI-DSS - généralement de taille modeste, son bon fonctionnement permet néanmoins la bonne circulation des paiements et de certains échanges financiers avec les partenaires

  SI Investissement : dans le monde bancaire, le SI investissement possède une importance particulière en termes de risques, en effet, même si la population employée est restreinte par rapport au réseau de distribution, ce SI produit généralement une grande part des bénéfices de l'organisation – il est généralement centralisé au niveau du groupe et suit des règles de gestion et de séparation des pouvoirs particulières

Face à ce SI, ou plutôt ces SI multifacettes, l'organisation financière se doit de gérer un challenge complexe quant à la sécurité opérationnelle et stratégique. L'activité des officiers de sécurité garants du SI se caractérise alors par une veille technique intense, une bonne compréhension des tactiques d'attaques et l'invention continuelle de contremesures adéquates pour le protéger. Il est donc essentiel de connaitre les types d'attaques qui sont exécutées vers les institutions financières.

QUELS TYPES D'ATTAQUES POUR LES SI FINANCIERS ?

Évidemment, la plupart des attaques « classiques » connues peuvent être exécutées sur les SI des institutions financières, mais comme nous l'avons vu précédemment, les SIs financiers proposent des caractéristiques propres qui exposent des risques et des enjeux différents si on les compare aux SIs industriels ou aux SIs des grands distributeurs par exemple. Dans le monde bancaire ou assurance, selon le sous-SI visé, les attaques peuvent varier mais il est néanmoins possible de répertorier les attaques les plus communes :

- **Déni de Services (DDoS) :** il s'agit de l'attaque la plus commune, impactant principalement le SI du réseau du distribution – impact immédiat, visant généralement à compromettre la réputation de l'établissement – il est à noter que certaines attaques DDoS ont historiquement visé le système monétique afin de bloquer certains échanges
- **Code malicieux sur les points de vente et systèmes de retrait :** ces attaques peuvent prendre plusieurs formes : malware spécifique permettant d'intercepter les données, injections de données, copie des moyens de paiement, etc.
- **Malware sur le système d'information :** ici, il n'y a généralement rien de spécifique quant à l'environnement bancaire ou assurance, même si les récentes attaques mettent en lumière la création de malware spécifiques aux environnement financiers afin de maximiser l'impact et l'efficience de l'attaque – il s'agit ici d'infecter directement le sous-SI considéré afin d'accéder aux données de celui-ci
- **Menace d'initié (Insider Threat) :** les employés peuvent directement mener des opérations frauduleuses volontaires ou involontaires. Dans le cas d'une action volontaire, l'élévation de privilèges et le mouvement latéral sur les systèmes Windows est généralement utilisé.
- **Phishing :** cette attaque peut exister sous deux angles, aux objectifs bien différents : **(1)** Phishing visant les usagers, extrêmement répandue, cette attaque vise directement les usagers des services financiers, les inondant d'emails plus ou moins bien formatés visant à récupérer leur identité financière digitale et ainsi réaliser en aval des opérations en leur nom. **(2)** Phishing visant le sous-SI de l'instruction financière, avec comme objectif principal l'injection d'une porte dérobée ou l'installation d'un malware pour prendre le contrôle d'une partie du sous-SI et exploiter les données métier au sein de l'établissement
- **Exploitation des vulnérabilités :** ces attaques utilisent directement les faiblesses de configuration du sous-SI ou le fait qu'il ne soit pas mis à jour régulièrement – ces attaques visent principalement les vulnérabilité Windows et Active Directory dans l'objectif à nouveau de maximiser les chances de réussites ainsi que le retour sur investissement de l'attaque

L'ensemble de ces différentes méthodes d'attaque ont pu être répertoriées depuis environ trois ans dans de nombreux pays différents et dans des institutions de tailles extrêmement variées.

QUELQUES EXEMPLES RÉCENTS

Le monde financier est par nature discret sur les mécaniques précises des attaques constatées ou repérées. Il existe néanmoins des exemples connus d'attaques ayant impacté fortement certaines organisations :

- En 2018, les codes malicieux FASTCash et ATMJackPot permettent aux attaquants de dérober directement de l'argent depuis les systèmes de retrait de type ATM
- En 2018, les malwares Carbanak et Cobalt visent plus d'une centaine d'institutions financières dans plus de quarante pays résultant un vol de plus d'un Milliard d'Euros. Ces malwares ont une couverture étendue, ils s'installent sur les SI ou sous-SI des organisations et permettent de manipuler des comptes bancaires, de définir des transferts frauduleux mais aussi de contrôler certains points de retrait (ATMs)
- En 2019, la banque américaine Capital One est soumise à un vol de données personnelles révélant les informations sur plus de cent millions de clients (noms, revenus, numéros de téléphone, emails, etc.)
- En 2019, la société financière Mouvement Desjardins révèle qu'une attaque interne menée par un employé a abouti au vol d'informations concernant presque trois millions de membres particuliers ou entreprises
- En 2019, la banque Dutch Bangla Bank Limited a été la victime d'une attaque externe au travers des systèmes de retrait en Russie et en Ukraine, provoquant le vol de plus de trois millions de dollars et d'une chute de réputation exceptionnelle

Et la liste est encore longue...

QUELLES CONTREMESURES METTRE EN ŒUVRE ?

Considérant le modèle distribué des SIs financiers, il est de fait extrêmement complexe de déployer une politique de sécurité à 360 au travers de l'organisation. Nous pouvons néanmoins vous conseiller l'implémentation immédiate des actions suivantes :

- Étudiez les modèles d'attaques de votre secteur et investissez dans les équipes de type Red Team qui simuleront des attaques ciblées en adéquation avec les particularités du secteur bancaire ou assurance : formez vos équipes, faites-les monter en compétence et réalisez régulièrement des tests d'intrusion et de vol de données
- Intégrez le modèle MITRE ATT&CK dans votre schéma d'étude : ce modèle est actuellement le plus complet et le plus adapté aux attaques modernes, il vous permettra de mieux comprendre la complexité des attaques et de construire votre propre schéma de contre-mesures adaptées
- Veillez aux vulnérabilités les plus courantes : patchez vos systèmes, auditez les changements sur les systèmes sensibles et surveillez les actions des comptes à pouvoir
- Gérez la particularité Active Directory : la plupart des designs Active Directory ont été réalisés il y a une dizaine d'années, à une époque où les attaques ciblées de malware et les méthodes modernes de phishing n'existaient pas – vous devez traiter le cas Active Directory avec un plan d'actions particulier

LE CAS PARTICULIER D'ACTIVE DIRECTORY

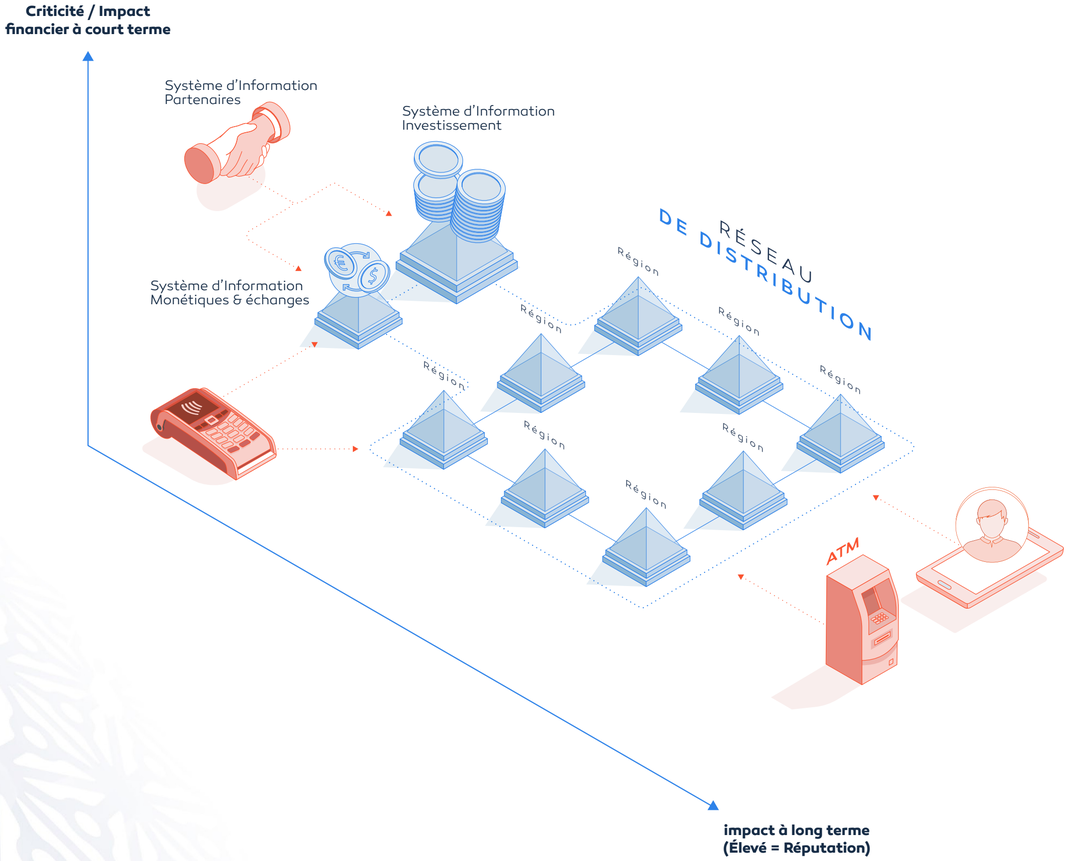
Pourquoi Active Directory représente-t-il une menace latente pour la plupart des organisations ?

L'environnement Active Directory offre un terrain de jeu particulièrement favorable aux attaquants ou malwares, et ce pour plusieurs raisons :

- Une communication incomplète de la part de Microsoft à propos de la sécurité Active Directory avec notamment une sortie trop tardive des documents décrivant le design de type tier-model
- La plupart des designs Active Directory actuellement en production ont plus de 10 ans, la mise à jour régulière des contrôleurs de domaine ne permet pas de corriger le design initial
- Depuis 2015, l'explosion des malwares spécifiques à Active Directory lors des attaques ciblées se combine avec une efficacité grandissante des groupes de hackers
- La couverture d'Active Directory est exceptionnelle pour un attaquant car cet annuaire est utilisé dans plus de 95% des organisations qui possèdent plus de 50 PCsv

Pour compléter votre réflexion, nous vous conseillons la lecture d'un article extrêmement intéressant **« Why Hackers Abuse Active Directory »** du site BankInfoSecurity.com. Cet article explique de manière très didactique pourquoi les attaquants ciblent particulièrement Active Directory pour arriver à leur fin, notamment dans les diverses institutions financières. Vous pouvez retrouver cet article ici :

https://bit.ly/2LS34gT



Active Directory : une cible de choix dans le monde bancaire

Nous pouvons projeter l'usage d'Active Directory dans les différents sous-SI financiers selon le schéma suivant :

Il existe donc généralement de nombreuses forêts Active Directory dans les différents sous-SI, avec dans la plupart des cas des relations d'approbation permettant le mécanisme de SSO pour certains utilisateurs.

Très souvent, le réseau de distribution possède de nombreuses forêts, historiquement héritées des anciennes organisations régionales. Ces forêts Active Directory comportent parfois des niveaux de maturité et de sécurité extrêmement hétérogènes. Il s'agit généralement des bases de données Active Directory les plus larges et les plus complexes, car de nombreux personnels travaillent sur ces entités distribuées.

La plupart du temps, le SI Investissement englobe une ou plusieurs forêts, généralement à l'échelle mondiale, notamment pour gérer les différentes places de marché ou des lieux d'investissement variés. Il n'est pas rare de constater une forêt par plaque : Amérique, Europe et Asie, avec des relations d'approbations entrantes et sortantes pour chacune des forêts.

Pour finir, le SI Monétique possède généralement sa propre forêt, notamment pour être en capacité de gérer les spécificités obligatoires des règles de conformité PCI-DSS, axe fortement structurant dans les SIs monétiques. La forêt monétique est très souvent coupée du reste du SI, en évitant des relations d'approbation avec les autres environnements Active Directory de l'organisation.

L'ensemble de ces caractéristiques spécifiques aux institutions financières et bancaires : multiplicité des sous-SIs, modèle distribué d'Active Directory, multiplicité des forêts, relations d'approbation nombreuses et des designs Active Directory parfois anciens représentent un environnement particulièrement propice aux attaquants désirant prendre le contrôle de votre système d'information.

Sécuriser Active Directory, une urgence pour les organisations du secteur bancaire ou assurance

La diversité des activités et le modèle distribué des institutions financières représentent donc des particularités extrêmement intéressantes pour les attaquants ; il convient donc de mettre en œuvre les contre-mesures adéquates pour se protéger convenablement.

Les institutions financières doivent prendre en compte trois dimensions dans leur protection Active Directory :

- Vérifier la configuration en amont : vérifier selon un plan continu la bonne configuration du service Active Directory, avec plusieurs milliers de changement par jour dans l'annuaire, il s'agit d'une tache de fond absolument nécessaire
- Mettre un œuvre un plan de détection des attaques : l'annuaire Active Directory étant sensible à des attaques spécifiques et évoluées, il convient d'être en mesure de détecter ces attaques ciblées en utilisant des solutions dédiées à l'environnement Active Directory
- Etre en mesure de connaitre l'ensemble des modifications réalisées dans l'annuaire en cas d'exécution d'un plan de remédiation : en cas d'attaque avérée l'institution doit être capable de connaitre l'ensemble des modifications réalisées dans l'intervalle d'attaque afin d'exécuter un plan de remédiation et éventuellement remonter à la source de l'attaque (patient zéro)

QUELLE EST LA PROCHAINE ÉTAPE ?

Comme nous l'avons évoqué au travers de ce document, les institutions financières, de par les spécificités de leur SI sont particulièrement sensibles aux attaques utilisant Active Directory. La protection contre ces attaques sera un élément majeur de la sécurité des banques et assurances dans les mois à venir.

Il convient donc de prendre en compte ce paradigme et de mettre un plan d'actions afin d'éviter la fuite de données ou pire, une chute de confiance envers l'institution elle-même.

Pour aller plus loin dans vos recherches et améliorer votre plan continu de sécurité, Alsid met à disposition sur son site web de nombreuses explications et livres blancs vous permettant de trouver quelques inspirations supplémentaires www.alsid.com