AYI NEDJIMI Consultants

Insider threat cyber : quand vos défenseurs travaillent pour l adversaire

Catégorie : Cybersécurité Générale Lecture : 4 min Publié le : 28/03/2026 Auteur : Ayi NEDJIMI

Insider threat en cybersécurité : deux experts plaident coupable comme affiliés BlackCat. Analyse du risque et recommandations pour les RSSI.

Deux experts en cybersécurité viennent de plaider coupable pour avoir opéré comme affiliés du ransomware BlackCat. L un était incident responder, l autre négociait les rançons côté victimes. Ce n est pas un scénario de film — c est la réalité d un secteur qui doit urgemment repenser la confiance accordée à ses propres professionnels. Et si le maillon faible de votre sécurité, c était celui que vous payez pour la garantir ? Insider threat en cybersécurité : deux experts plaident coupable comme affiliés BlackCat. Analyse du risque et recommandations pour les RSSI. Ce guide couvre les aspects essentiels de insider threat cybersécurité : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

Le mythe du défenseur infaillible

Dans la cybersécurité, on passe beaucoup de temps à modéliser les menaces externes. APT étatiques, cybercriminels, hacktivistes — on les cartographie, on les profile, on construit des défenses contre eux. Mais la menace interne reste le parent pauvre de la plupart des stratégies de sécurité.

L affaire Goldberg-Martin devrait servir d électrochoc. Ryan Goldberg, responsable réponse à incidents chez Sygnia, avait accès aux systèmes les plus critiques de ses clients. Kevin Martin négociait les rançons chez DigitalMint — il connaissait les seuils de douleur financière des victimes. Ensemble, ils ont ciblé cinq entreprises dont trois hôpitaux, causant 9,5 millions de dollars de dégâts. L expertise qui devait protéger les victimes a été retournée contre elles.

Un problème structurel, pas un incident isolé

Ce n est pas la première fois. En 2024, un analyste SOC d une grande ESN européenne avait été identifié comme revendeur d accès initiaux sur un forum russophone. En 2023, un pentester australien avait été condamné pour avoir exploité les failles qu il découvrait en mission pour exfiltrer des données à son profit. Le secteur de la cybersécurité souffre d un paradoxe fondamental : les personnes les mieux placées pour protéger sont aussi les mieux placées pour attaquer.

Le problème est structurel. Le marché du travail cyber est tellement tendu que les vérifications d antécédents sont souvent superficielles. Les certifications techniques (OSCP, CISSP) valident des compétences, pas une éthique. Et la pénurie de talents pousse les entreprises à accorder des niveaux d accès disproportionnés à des prestataires qu elles connaissent à peine.

Ce que ça change pour les RSSI

Si vous êtes RSSI ou DSI, cette affaire devrait vous amener à revoir trois points précis dans votre dispositif :

1. La compartimentation des accès prestataires. Un consultant en réponse à incidents n a pas besoin d un accès permanent à votre AD, votre SIEM et vos sauvegardes simultanément. Accès limités dans le temps, journalisés, révocables en un clic. C est basique, mais combien d entre vous le font réellement ?

2. La séparation des rôles dans la gestion de crise. L entreprise qui négocie votre rançon ne devrait jamais être celle qui a accès à vos systèmes internes. La tentation est trop grande, et l affaire BlackCat le prouve. Deux prestataires distincts, deux périmètres étanches.

3. La surveillance des surveillants. Vos outils de détection surveillent les utilisateurs métier, les admins système, les VPN. Mais surveillent-ils les comptes des consultants sécurité eux-mêmes ? Les EDR détectent-ils une exfiltration depuis le poste d un pentester mandaté ? Dans la plupart des cas, la réponse est non — ces comptes sont en liste blanche.

Le vrai sujet : la confiance vérifiable

La solution n est pas la paranoïa généralisée. Le secteur ne fonctionnera pas si chaque client soupçonne chaque prestataire. La solution, c est de passer d une confiance implicite à une confiance vérifiable. Des audits croisés réguliers. Des clauses contractuelles avec pénalités réelles. Des systèmes de journalisation que le prestataire lui-même ne peut pas désactiver. Et surtout, une culture où signaler un comportement suspect d un collègue ou d un partenaire n est pas vu comme de la délation, mais comme un acte de responsabilité professionnelle.

Mon avis d expert
L affaire BlackCat est un symptôme d un secteur qui grandit trop vite. On recrute massivement, on forme en accéléré, on accorde des accès critiques à des profils qu on ne connaît pas assez. Je ne dis pas qu il faut ralentir — la menace n attend pas. Mais il faut industrialiser la vérification. Le zero trust ne doit pas s appliquer uniquement aux machines et aux réseaux. Il doit s appliquer aux humains aussi, y compris — surtout — à ceux qui portent le titre de "expert en cybersécurité". C est inconfortable, mais c est nécessaire.

Sources et références : CERT-FR · MITRE ATT&CK

Articles connexes

- Top 10 Outils Sécurité - Guide Pratique Cybersecurite
- Ransomware Trends Q1 2026 : Analyse des Groupes en 2026
- Livre Blanc : Sécurisation | Threat Intelligence 2026

- Top 10 Solutions EDR/XDR | Threat Intelligence 2026

Conclusion

L insider threat n est pas un risque théorique réservé aux rapports d analystes. C est un risque opérationnel qui vient de se matérialiser de la pire manière possible : par ceux qui étaient censés nous protéger. Chaque RSSI devrait se poser la question aujourd hui : si l un de mes prestataires sécurité basculait demain, quels dégâts pourrait-il causer avec les accès dont il dispose actuellement ? Si la réponse vous inquiète, c est qu il est temps d agir.

Points clés à retenir

- Le mythe du défenseur infaillible
- Un problème structurel, pas un incident isolé
- Ce que ça change pour les RSSI
- Le vrai sujet : la confiance vérifiable
- Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr