Exposition à une vulnérabilité de type « exécution de code arbitraire »

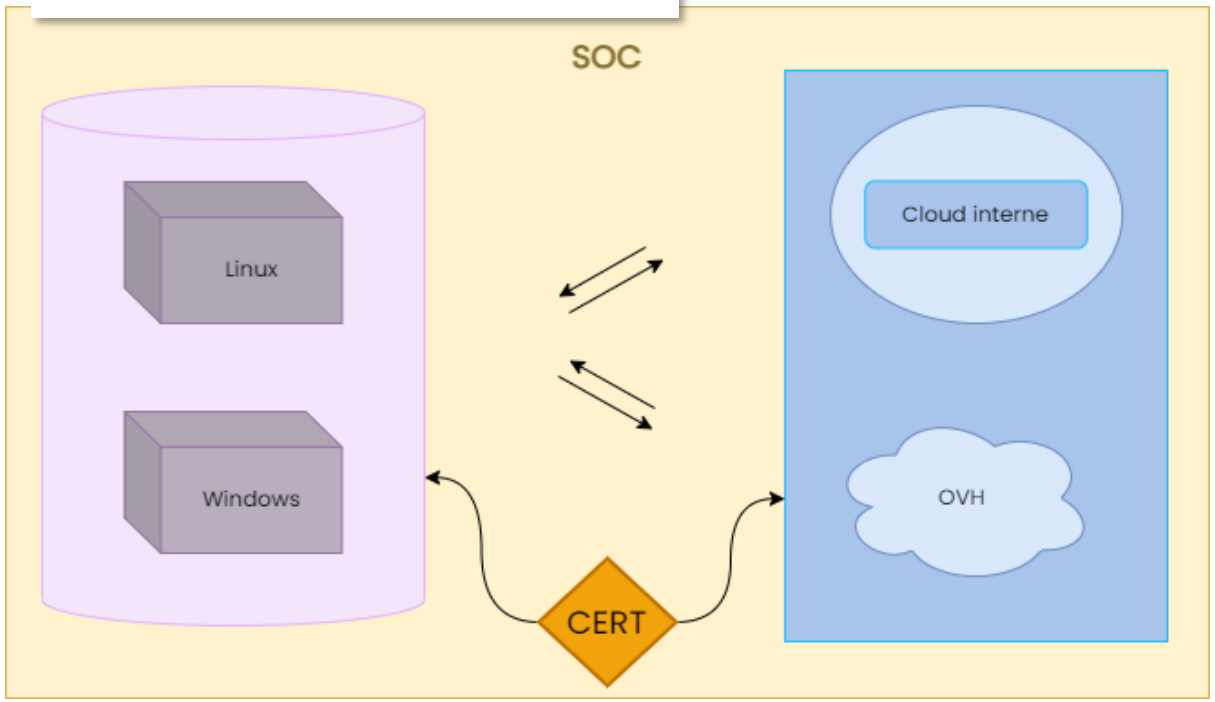
1) Gestion de la vulnérabilité
    a. De quel type de vulnérabilité s'agit-il ?
    b. Quels sont les risques à cantonner en cas d'exploitation de la vulnérabilité
2) Gestion de crise
    a. Plan de gestion de crise en cas d'exploitation de la vulnérabilité
    b. Exercice «ACE 1»

1) Gestion de la vulnérabilité

Nature de la vulnérabilité

Les vulnérabilités de type « exécution de code arbitraire » consiste en **l'exécution de commande, par injection de code sur une machine cible ou sur un processus cible sans y être autorisé**. Elles font donc partie d'un ensemble de failles de sécurité critiques qui pourrait exposer NewTech à de graves crises liés à des problématiques sur le patrimoine informationnel, économiques, juridiques, stratégiques.

Infrastructure de NewTech



- NewTech bénéficie de serveurs tournant sur deux systèmes, ce qui donne la possibilité d'assurer une continuité de l'activité, en cas de vulnérabilité sur un des deux systèmes.
- Les solutions de cloud hybride ajoutent des enjeux sécuritaires, dans la communication avec le datacenter et les 700 collaborateurs
- Le CERT et SOC en collaboration avec un partenaire externe permet une surveillance globale sur le système, et sur l'identification des risques

1) Gestion de la vulnérabilité

Les impacts à limiter (1/2)

1. **Surveiller** les accès en tant qu'administrateur

Dans le cas d'une vulnérabilité d'exécution de code arbitraire, l'attaquant pourrait s'emparer du contrôle de plusieurs machines connectés au même réseau, et se doter d'un droit de super user.

Dans le cas d'une telle élévation des privilèges, il pourrait donc arriver qu'une machine atteinte par l'attaquant télécharge des fichiers, ou des logiciels non approuvés.

Cet accès non autorisé aux droits d'administrateurs peut engendrer une cascade de conséquences qui pourrait se révéler critique dans la pérennité de NewTech (vol de données, newTech comme plateforme pour infecter tous les collaborateurs ainsi que leurs équipements).

2. **Contrôler** la confidentialité

La possession de NewTech de données personnelles s'avère être un enjeu énorme pour la crédibilité de l'entreprise sur le marché, un enjeu pour se démarquer de ses concurrents.

Estimer à quel point la confidentialité de documents est entravée est vital pour mesurer les impacts juridiques et stratégiques en cas de divulgation. Ces violations de confidentialité peuvent atteindre un serveur Linux sur lequel est exploité la vulnérabilité, mais peut aussi s'entendre sur l'ensemble des serveurs vulnérables, ainsi que sur les machines connectées au même réseau, bien qu'elles soient insensible à cette faille.

Identifier les motivations et les origines de l'attaque est aussi utile pour anticiper les conséquences d'une divulgation de documents confidentiel. Les réutilisations malveillantes sont multiples : revente sur le marché noir, espionnage...

3. **Prévenir** les risques d'immobilisation des activités et services de NewTech

Dans le cas de l'exploitation de la vulnérabilité en question, le risque d'attaque par Déni de service est fort, impliquant des graves conséquences sur l'indisponibilité des applications et des services de NewTech, pour les partenaires et pour les clients. En effet, les attaques de ce type peuvent compromettre la fiabilité des serveurs. L'endiguement des attaques s'avère être un moyen efficace pour maximiser la fiabilité des serveurs.

1) Gestion de la vulnérabilité

Les impacts à limiter (2/2)

4. Evaluer l'intégrité de la donnée

L'accession aux droits de super utilisateurs pour un attaquant peut aussi mettre en danger l'intégrité des données détenues par NewTech.

A ce stade, plusieurs options pour l'attaquant sont possibles :

- Suppression de données
- Modification de données
- Création de faux fichiers

Tous ces options peuvent affecter les services et les collaborateurs sur le court, moyen et long terme. La suppression de données doit être au centre de toutes les attentions car il immobiliserait immédiatement les activités des parties prenantes de NewTech (mails, rapports, compte rendus…).

Les sauvegardes sur des serveurs isolés du réseau sont à considérer pour anticiper une telle attaque qui pourrait compromettre l'intégrité des données de l'entreprise

5. Limiter la propagation de l'attaque chez les partenaires de NewTech

La portée de la vulnérabilité ne se limite malheureusement pas aux serveurs Linux vulnérables. En effet, en partant d'une machine sensible à cette vulnérabilité d'exécution de code arbitraire, l'attaquant pourrait aussi procéder à l'envoi de données sur les des postes de travail, pour les infecter à leur tour, et prendre possession de l'ensemble de l'infrastructure.

A partir de cette hypothèse, les possibilités pour l'attaquant sont très larges : la propagation de l'attaque chez les partenaires de NewTech pour n'en citer qu'une.

Cette propagation peut être réalisée suivant plusieurs procédés : l'envoi de spam d'email, l'utilisation des machines infectés pour réaliser des attaques sur les sites internet tiers, ou s'emparer de données appartenant aux partenaires, qui sont censées rester au sein de NewTech.

Des mesures d'anticipation comme le filtrage et le cloisonnements du réseau doivent être mises en œuvre pour tempérer ces impacts qui pourrait nuire grandement à la réputation de NewTech

1) Gestion de crise

Plan d'action de gestion de crise (1/4)

Dans le cas où la vulnérabilité viendrait à être exploitée à des fins malveillante. Il est essentiel pour NewTech de créer une cellule en interne de gestion de crise, pour **palier aux attaques, limiter la propagation des attaques** et **protéger les ressources de NewTech.**

1. Alerter et mobiliser les parties prenantes

Dès les premiers signes confirmés d'une anomalie, et avant même l'application d'un correctif sous la direction du CERT, des messages d'alerte à toutes les parties prenantes interne doivent être envoyés. Une nouvelle politique de sécurité d'urgence doit être établie et envoyée aux partenaires. L'objectif est de raviver l'état d'alerte chez collaborateur pour éviter les phénomènes de propagation involontaires, mais aussi permettre la continuité des activités de NewTech (dans le cas d'une attaque généralisée qui pourrait atteindre l'ensemble de l'infrastructure).

Les équipes IT et les responsables du SOC doivent être réunis et sous la décision du RSSI/DSI doivent former une cellule de crise dans une salle à part, avec les tous les moyens et autorisations nécessaires pour agir sur n'importe quelle machine du réseau.

2. Comprendre l'attaque et ses motivations

Il est capital de comprendre le chemin de l'attaquant pour comprendre ses motivations et les potentiels desseins. En mettant le SOC à contribution sur l'identification de l'attaquant, les conditions et les facteurs de la réussite de son infiltration dans le système, la cellule de crise pourrait même identifier la ou les machines qui sont atteintes, et suspendre leur activité, pour éviter une propagation.

Plan d'action de gestion de crise (2/4)

3. Durcir le système d'information

Agir sur le DIC (Disponibilité, confidentialité, intégrité)

Dans le cas d'une crise de cette envergure, il est essentiel de focaliser les efforts sur les trois principaux enjeux :

La disponibilité : L'accès à la donnée doit être possible uniquement par les personnes spécifiquement autorisées, dans le respect des plages horaires d'utilisation prévues

La confidentialité : Création d'une hiérarchisation des autorisations, dans l'accès aux données sensibles de NewTech

L'intégrité : Mobiliser le SOC sur l'exactitude des biens et des informations. Il doit détecter toute modification, création ou suppression inhabituelle de biens informationnels appartenant à NewTech et ses partenaires.

Application maitrisée du modèle zéro trust

Le modèle de sécurité actuel de NewTech doit s'inspirer du modèle zéro trust, visant à réduire la confiance implicite accordée aux utilisateurs. Les équipements tels que les pare feux et proxies sont conservés mais un cloisonnement des ressources doit être appliqué :

Les utilisateurs doivent bénéficier des autorisations minimales pour réaliser leurs activités. De plus les moyens d'authentifications doivent être renforcés, avec une solution d'authentification à doubles facteurs par exemple ou MFA.

Enfin Les flux doivent être chiffrés avec l'utilisation des protocoles TLS

Mise en place de CASB

L'objectif est de sécuriser les applications SaaS et IaaS ainsi que les données qui y transitent. L'utilisation du cloud hybride chez NewTech peut être une opportunité d'attaque, d'où la mise en place d'un Cloud Access Security Broker (CASB) qui va sécuriser les données entre le cloud vers les périphériques en :

- Contrôlant les accès des utilisateurs et analyser leurs activités
- Alertant sur les menaces et détectant tout type de logiciel malveillant
- Améliorant la visibilité sur les applications cloud de NewTech
- Détectant tout comportement suspect, shadow IT…

Plan d'action de gestion de crise (3/4)

3. Durcir le système d'information

Diminuer l'impact en réduisant le risque et la probabilité d'une potentielle nouvelle attaque

En assurant le bon filtrage des ports d'administration, en segmentant le réseau et en mettant en place des modèles de cloisonnement entre Internet et le reste du système d'information (modèle «forteresse» par exemple[1])

Il faut aussi établir ou s'assurer si les équipes l'ont déjà mis en œuvre la bonne redondance des données en suivant la règle du 3-2-1 de la sauvegarde (trois copies des données, un sur le Cloud, un dans les serveurs Windows non vulnérables à la faille en question, avec une copie des données hors site et hors ligne)

L'étape de chiffrement des données doit être réalisé en priorité sur les serveurs les plus à risques à savoir les serveurs linux

Refonder les solutions de gestion des accès à privilèges

Il est aussi nécessaire de refonder la gestion des privilèges des utilisateurs, par des solutions PAM permettant une protection relativement complète pour les comptes utilisateurs possédant de forts privilèges.

L'objectif de la mise en place d'un tel dispositif est de limiter plusieurs menaces en interne comme des partages de mots de passes, mais aussi externe en cantonnant des potentielles compromissions de prestataires.

Une solution PAM centralise les accès à hauts privilèges et empêche les connexions directes aux équipements, ce qui préviendrait considérablement un bon nombre de types d'attaques. Il faut mobiliser le SOC et les équipes gérant la crise sur la création de bastions, coffre-fort de mots de passes, de portails d'accès pour sécuriser les accès externes

1 : https://www.ssi.gouv.fr/uploads/2021/08/anssi-article-systemes_information_hybrides_et_securite_un_retour_a_la_realite.pdf Figure 1.1

Gestion de crise

Plan d'action de gestion de crise (4/4)

4. Communiquer habilement en interne et externe

Parmi les premières choses à faire en cas d'attaque de cette envergure, qui pourrait fragiliser non seulement les parties prenantes internes de NewTech, mais aussi externes, avertir les équipes est une étape prioritaire, pour endiguer et limiter la propagation de l'attaque. L'objectif est double :

- Préventif : mettre l'ensemble des équipes en état d'alerte pour augmenter la vigilance. Plusieurs éléments doivent être transmis :
  - L'attaque en question est critique, mais maitrisée par une équipe compétente
  - N'ouvrir que les mails de confiance
  - Changer les mots de passes
  - Ne connecter aucun périphérique personnel sur les postes de travail pour limiter les propagations d'infection
- Maintenir la confiance : montrer que le SOC et les équipes sont mobilisés pour gérer la crise, et que la continuité des activités de NewTech peut être assurée.

5. Tirer des leçons de la crise et capitaliser

Pour assurer une reprise d'activité sereine, NewTech doit planifier un plan de sortie de crise. Le CERT doit être mobilisé au plus haut à la fois pour donner un correctif le plus rapidement, et d'autre part pour ne pas prolonger la crise inutilement et utiliser des ressources pour rien.

Les leçons doivent être tirées à chaud mais aussi plusieurs semaines après pour tirer profit de la crise et affiner les processus de gestion de crise pour qu'ils soient plus adaptés à NewTech, et donc lui permettre d'être plus réactif, dans l'objectif de réduire au maximum les dégâts matériels, humains, informationnels

Exercice de gestion de crise

Cadre et objectifs de l'exercice

Nom de l'exercice : ACE 1

Durée : 8h30 Plage horaire : Matin/Après-midi

Niveau des joueurs : Cellule de crise décisionnelle de NewTech + cellule de crise de SecurOperator

Thème : Attaque par l'exploitation de vulnérabilité de type exécution de code arbitraire

Joueurs : Profils décisionnels, responsables IT, communicants

Planificateurs : DSI et RSSI de NewTech

Rôles à simuler

Interne	Public	Privé
Equipe technique et responsables métiers et communicants	ANSSI cybermalveillance.gouv.fr	Partenaires externes, OVH

5 objectifs

Sensibiliser les équipes sur l'importance d'une bonne hygiène du SI

Fédérer les différentes équipes IT et améliorer leur efficacité en groupe

Se préparer à des situations critiques qui immobiliserait l'activité de NewTech

Former les équipes sur les restauration de données, la protection à un grand nombre d'attaque en même temps, développer l'expertise et le savoir faire

Tester un premier dispositif de gestion de crise, et en déduire l'importance

Exercice de gestion de crise

Scénario (1/2)

Alerte et détection des premières anomalies

A **8h00,** des premiers messages d'incidents sont remontés auprès des responsables IT, et signalés auprès du RSSI. Des problèmes de disponibilité de la donnée ne permettent plus aux partenaires, aux collaborateurs internes de NewTech de continuer leurs activités. A 9h00, des utilisateurs voient leur compte supprimés, et leurs fichiers stockés sur leurs comptes supprimés.

Pression des partenaires

A **10h,** l'anomalie est constatée et repérée sur les serveurs Linux. Des premières stratégies d'endiguement doivent être prises. Plusieurs messages et appels de la part des partenaires de NewTech interpellent sur la gravité de la situation. Des premiers messages de prévention sont envoyés aux partenaires et aux équipes internes « viriles », dans l'idée de maintenir la confiance et de redoubler la vigilance. A **12h**, l'incident est remonté à l'ANSSI dans le but de recevoir des indications concernant la protection du SI. A **12h15**, OVH signale plusieurs problèmes sur ses serveurs Linux.

Pression des clients

A **12h30**, de nombreux clients se plaignent de ne pas recevoir des alertes, des mails. A **12h40**, des données confidentielles sont publiées sur Internet. Des menaces juridiques sont avancées.
A **14h**, l'ANSSI reporte bien la vulnérabilité et transmet des recommandations. Le CERT est mobilisé.

Exercice de gestion de crise

Scénario (2/2)

Propagation de l'attaque sur des serveurs non vulnérables

A **15h**, des serveurs Windows et cloud sont infectés et voient leur intégrité compromise. Un serveur s'arrête brutalement. Une attaque DDoS s'attaque sur une partie des serveurs.
A **15h15**, le débit entrant est limité, et les politiques de confidentialités sont revues à la hausse. Les serveurs infectés sont coupés du réseau pour limiter la propagation du code malveillant.

Afflux conséquent de plaintes

A **16h**, une nouvelle plainte arrive toutes les 5 minutes pendant 2 heures, les données sont soit chiffrées, soit indisponibles, soit supprimées, soit erronées.
Les services de sauvegarde hors ligne sont mobilisés pour rétablir le plus rapidement possible les données intactes.

Remédiation et fin de l'exercice

A **17h**, des premiers résultats sont donnés, les sauvegardes hors ligne sont partiellement impactées, et les outils en ligne sont toujours indisponibles.
La pression continue venant de plusieurs acteurs et partenaires. La cellule de crise établit une stratégie pour les deux prochaines semaines, dans le but de revenir progressivement à la normale.
Fin de l'exercice à **18h30**, avec RETEX à chaud prévu pour faire le point sur les difficultés rencontrées.