< Seuils et Alertes >

Cas d’usage #1
Fiche Réflexe

Groupe de travail gestion de crise et entraînement

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CDSE CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

AMRAE la Maison du risk management

CESIN

BANQUE DE FRANCE EUROSYSTÈME

CLUSIF

CCA Club de la Continuité d'Activité

Cette fiche présente les cas d'usages qui ont semblé au groupe de travail les plus importants à traiter : scénario d'un **rançongiciel** ; scénario d'une **vulnérabilité dite "0 day"**. En effet :

- Une suspicion de rançongiciel ou la confirmation d'un rançongiciel impose une réaction immédiate et forte pour protéger les systèmes d'informations. Cette situation est exceptionnelle pour une organisation mais les impacts très importants.
- La mise en place d'un correctif à la suite d'une publication d'une vulnérabilité peut nécessiter une réactivité et une mobilisation forte en fonction de la gravité, de la vulnérabilité et du volume d'actifs concernés. Cette situation devient courante dans les organisations, et les impacts ne sont pas immédiats sur les systèmes d'information.

< Scénario Rançongiciel >

Scénario : Un écran rouge avec un décompte et des têtes de mort s'affichent sur les postes de travail de votre entreprise.

Scénario : Des ralentissements sont constatés sur les postes de travail et l'accès aux applicatifs du système d'information.

Contexte interne

Mardi, 7 h 45. Le centre de services reçoit une salve d'appels : des postes redémarrent en boucle, un message rouge affirme que « vos fichiers sont chiffrés » et un compte à rebours de 72 h s'affiche. Dans la même heure :

- Les sauvegardes de la nuit échouent pour le serveur de fichiers ;
- Le logiciel qui surveille les actes malveillants sur les postes de travail et les serveurs fait remonter un pic d'écritures sur l'extension *.lock ;
- L'équipe ou le prestataire en charge de la surveillance continu des alertes de sécurité constate une brutale envolée du trafic SMB [1]et RDP [2]latéral ;
- La supervision métier signale l'indisponibilité de l'ERP [3]logistique.

Un examen rapide prouve que le contrôleur de domaine a été touché : les stratégies de groupe ont poussé un binaire suspect signé « svchost.exe ». L'attaquant a également désactivé les clichés instantanés de volumes (VSS) et tenté d'effacer les tâches de sauvegarde hors ligne. Les sauvegardes restées déconnectées physiquement deviennent donc critiques.

[1] Server Message Block (SMB) est un protocole permettant le partage de ressources sur des réseaux
[2] Remote Desktop Protocol (RDP) : Protocole permettant à un utilisateur de se connecter à un service Microsoft Terminal Server
[3] Enterprise Resource Planning : Progiciel permettant la gestion des processus de l'entreprise

Chronologie interne (≤ 3 h)

- T + 0 h : Détection des premiers postes chiffrés, isolement réseau d'un segment bureautique.
- T + 0 h 30 : Confirmation que le contrôleur de domaine télécharge un binaire depuis un dépôt GitHub éphémère ; coupure d'urgence du réseau « user ».
- T + 1 h : Cellule de crise convoquée ; décision de débrancher les baies de sauvegarde hors ligne pour prévenir tout chiffrement différé.
- T + 2 h : Évaluation RGPD : présence potentielle de données RH sensibles ; le DPO pré-alerte la CNIL.
- T + 3 h : Début de reconstruction d'un domaine « clean » parallèle sur site de secours ; déclenchement du PRA pour les applications critiques.

Exemples :

	NotPetya – 27 juin 2017	**LockBit – Royal Mail, 11 janv. 2023**
Critères d'alerte déclenchés	**Alerte technique :** 1/ Propagation ultra-rapide via partages Windows. 2/ Redémarrages en chaîne, table de partition corrompue. 3/ Sauvegardes locales chiffrées. **Alerte opérationnelle :** 1/ Arrêt de la facturation (Maersk). 2/ 45 000 postes paralysés. **Alerte réglementaire** : 1/ Si exfiltration de données personnelles, pré-alerte CNIL 2/ signalement auprès de l'ANSSI et de toute autorité régulatrice	**Alerte technique :** 1/ Chiffrement du serveur d'appui logistique (impression douanière). 2/ Blocage des imprimantes ; échecs d'envoi colis internationaux. 3/ Message de rançon affiché sur terminaux. **Alerte opérationnelle :** 1/ Suspension totale des exportations colis durant 3 semaines. 2/ Image de marque dégradée, pression médiatique. **Alerte réglementaire** : 1/ Si exfiltration de données personnelles, pré-alerte CNIL 2/ signalement auprès de l'ANSSI et de toute autorité régulatrice
Seuil atteint	**Alerte critique** : > 30 % du parc chiffré en < 30 min, serveurs AD et sauvegardes hors service, risque image et pertes > 10 Md $.	**Alerte renforcée** (tend vers critique) : processus métier unique mais vital bloqué ; note de rançon publique et menace d'exfiltration ; service national paralysé 20 jours

Niveau d'alerte mobilisé	**Niveau 3 – Cellule de crise mondiale** : activation DG, logistique, juridique, communication ; reconstruction d'un AD «ownCloud» resté éteint pour relancer le SI Maersk.	**Niveau 2+** : IT + Management + métiers logistiques puis cellule de crise ; décision de suspendre l'export colis et d'informer les régulateurs (ICO, Ofcom).
Commentaires / retours d'expérience	▪ Le rançongiciel était en réalité un ***wiper*** : paiement inutile. ▪ Les îlots réseau déconnectés (un seul contrôleur AD hors ligne) ont permis la reprise ; d'où l'importance de sauvegardes « froides » et segmentation. Litige cyber-assurance historique : 1,4 Md $ réglé en 2024, requalifié en « acte de guerre » par certains assureurs.	▪ Un seul maillon (impression douanière) suffit à bloquer l'activité. ▪ Processus papier de secours à documenter ***avant*** crise. ▪ Double extorsion : préparation d'un ***holding statement*** public jour 1 pour contenir la rumeur. • Test annuel de restauration des sauvegardes offline recommandé sur l'infra d'affranchissement.

- **NotPetya** coche tous les critères majeurs (techniques, opérationnels, réglementaires), dépasse largement les seuils « propagation » et « impact métier », et escalade instantanément au plus haut niveau de crise.
- **LockBit/Royal Mail** illustre qu'un seul service stratégique peut suffire à franchir le seuil « Alerte renforcée » ; l'indisponibilité prolongée et la médiatisation peuvent pousser au niveau 3 si l'exfiltration est confirmée.

Critères d'alerte	Les critères susceptibles d'influer sur l'évaluation de l'alerte sont : ▪ Une modification anormale (arrêt, purge, surcharge) sur un serveur d'annuaire **ou** de sauvegarde. ▪ Un ralentissement ou blocage simultané de plusieurs systèmes utilisateurs ou serveurs applicatifs. ▪ Le volume et la nature des systèmes touchés : postes utilisateurs isolés ? segment bureautique complet ? serveurs cœur de SI ? ▪ La détection d'exfiltration (double extorsion) : pics de transfert sortant, avertissement d'un CSIRT externe. L'intégrité des sauvegardes : présence d'échecs ou de chiffrage sur les référentiels de backup.

Seuils	En combinant les critères ci-dessus, on peut distinguer : ▪ **Alerte bénigne** – Chiffrement suspect d'un **poste isolé** ; sauvegarde saine disponible ; "***containment***" possible en < 15 min. ▪ **Alerte standard** – Plusieurs **postes** ou **un serveur non critique** atteints (< 5 % du parc) ; sauvegardes intactes. ▪ **Alerte renforcée** – Propagation à **plusieurs segments** ou à un **serveur critique** (contrôleur de domaine / ERP) ; début d'exfiltration. **Alerte critique** – Chiffrement/exfiltration **généralisée** : > 30 % du parc, sauvegardes corrompues, arrêt de production, demande publique de rançon.
Niveau d'alerte	On peut retenir trois niveaux[4] : ▪ **Alerte IT traitant** – Équipe SOC/EDR isole l'hôte et lance l'analyse. ▪ **Alerte IT traitant + IT Management** – Ajout du management IT, du responsable production et du DPO pour prioriser les ressources, décider d'éventuelles coupures réseau et préparer les notifications réglementaires (Ex. : CNIL ≤ 72 h ; ANSSI le plus rapidement possible ; ACPR ≤ 4 h ou 24h ; ...). **Alerte IT + Management + Cellule de crise** – Activation de la cellule de crise (Direction générale, Juridique, Communication, Métiers) ; déclenchement du PCA/PRA, gestion presse/partenaires, mobilisation de l'assurance-cyber (nécessité du dépôt de plainte sous 72H).
Commentaires	▪ **Mesure du rétablissement** : % de postes restaurés, RTO/RPO atteints, reprise des applications critiques. ▪ **Sauvegardes hors ligne** : tester immédiatement la restauration – ne pas attendre la fin du chiffrement. ▪ **Preuves** : conserver journaux EDR, instantanés hyperviseur, clés de registre avant toute réinstallation. ▪ **Communication** : préparer un message d'attente (« *holding statement* »), briefer l'assistance utilisateur pour éviter la désinformation. ▪ **Notifications réglementaires** : journaliser horodatage et contenu des envois (CNIL, ANSSI, ACPR, partenaires). **Assurance-cyber** : envisager l'assistance d'experts dès le niveau 2 si le contrat le permet.

[4] En miroir des niveaux préconisés par l'ANSSI : Technique, Opérationnel et Stratégique

Recommandations	▪ **Outillage** : Mettre en place des outils de détection d'attaques pour remonter une alerte technique au plus vite ▪ **Former/Entrainer** : Sensibiliser les utilisateurs au comportement pour bien réagir : savoir signaler, connaitre la consigne en cas de survenance **Sauvegarde** : Avoir une copie des données en mode déconnecté et analyser leur intégrité et tester la restauration régulièrement.

< Scénario vulnérabilité 0 day >

Scénario : Une vulnérabilité non exploitée touchant un grand nombre d'actifs est publiée et nécessite une mise à jour urgente des actifs concernés.

L'alerte initiale dans ce cas d'usage est généralement de nature technique.

La source de l'alerte peut être un éditeur de logiciel ou un constructeur, mais aussi un service de supervision ou une autorité comme l'ANSSI.

- Exemple de Log4j :

Le 9 décembre 2021, l'éditeur Apache Software Foundation a signalé une vulnérabilité dans le composant logiciel de journalisation sur Java, très utilisé dans les systèmes d'information. Le CERT FR a également publié une alerte le 16 décembre 2021 pour confirmer que la vulnérabilité était déjà largement utilisée de manière malveillante par des attaquants.

A réception de ce signalement, l'exploitabilité de cette vulnérabilité et également le volume d'actifs concernés (plusieurs milliers pour certaines) en fonction des organisations ont pu nécessiter la mobilisation des équipes pendant plusieurs jours, voire semaines, pour prioriser l'application des correctifs ou des contournements identifiés. Pour certaines, un dispositif de crise a été escaladé afin de mobiliser les ressources dans le temps et opérer un suivi de la maîtrise du risque d'exploitation de cette vulnérabilité. Des chaînes d'alertes se sont bien mises en place avec des objectifs de mobilisation avant tout.

Le tableau ci-dessous illustre une possibilité.

Critères d'alerte	Les critères susceptibles d'influer sur l'évaluation de l'alerte sont : - Le score de la vulnérabilité (ex : CVSS) : plus il est élevé, plus l'exploitation de la vulnérabilité est triviale et les impacts sont importants - L'existence d'une méthode d'exploitation activement utilisé (voire publiée sur Internet) - L'existence ou non d'un correctif, ou à minima d'une remédiation standardisée (ex : isolation d'un équipement) - Le volume d'actifs touchés par la vulnérabilité, leur nature et leur exposition (Internet, interne, isolé du réseau) La période depuis la publication (en source ouverte) de la vulnérabilité – plus elle est longue, plus la vulnérabilité est susceptible d'être exploitée
Seuils	En combinant les différents critères d'alerte, il est possible de considérer différents seuils. Voici une proposition : - Une **alerte bénigne** (par exemple, avec un score CVSS faible), qui sera traitée lors de la prochaine plage de maintenance prévue - Une **alerte standard** (par exemple, une alerte avec un score CVSS élevé touchant des actifs non exposés sur Internet et sans méthode d'exploitation connue) - Une **alerte renforcée** (par exemple, une alerte avec un score CVSS élevé sur des actifs exposés sur Internet mais sans méthode d'exploitation connue) - Une **alerte critique** (par exemple, une alerte avec un score CVSS élevé sur des actifs exposés sur Internet avec une méthode d'exploitation connue) Le volume d'assets peut également aider à définir un seuil complémentaire ou venir enrichir ceux proposés ci-dessus.

Niveau d'alerte	On peut par exemple imaginer 3 niveaux d'alerte :
	- Une alerte IT traitant
	  o L'objectif de cette alerte est de s'assurer d'assigner une action de correction à la personne en charge de l'équipement (propriétaire de la ressource).
	- Une alerte IT traitant + IT Management
	  o L'objectif de cette alerte est de
	  ▪ S'assurer d'assigner une action de correction à la personne en charge de l'équipement (propriétaire de la ressource), et

	▪ D'escalader le sujet aux responsables pour le bon niveau de priorisation - Une alerte IT traitant + IT Management + Cellule de crise o L'objectif de cette alerte est de ▪ S'assurer d'assigner une action de correction à la personne en charge de l'équipement (propriétaire de la ressource), et ▪ D'escalader le sujet aux responsables pour le bon niveau de priorisation De prévenir les métiers / le business d'un éventuel impact lors de l'application du correctif (ex : désactivation de fonctionnalité).
Commentaires	Il est important de mettre en place des moyens de suivi pouvant permettre de vérifier l'avancée du chantier en la matière : - Impact des mises à jour (***patch***) - % des actifs vulnérables traités
Recommandations	**Scanners de vulnérabilités** : outil permettant d'identifier les systèmes vulnérables afin de les isoler. **Bloquer les vecteurs d'exploitation** : Avoir une politique de mise à jour. **Gestion des accès systèmes** : Appliquer une approche "least privilege"

Annexe : Quelques bonnes pratiques complémentaires pour se préparer au mieux à ce type de scénarios ...

Axes	Recommandations
Prévention	Maintenir **les sauvegardes déconnectées** et testées mensuellement.
	Segmenter le réseau : production / bureautique.
Détection	Mettre en place une **supervision sécurité** adaptée : journalisation centralisée, alertes sur extensions inhabituelles.
	Sensibiliser les employés à signaler tout message suspect.
Réaction	Rédiger des procédures d'isolement poste/serveur (débranchement câble, arrêt WiFi).
	Disposer d'un « kit PRA » : comptes d'urgence, image système propre, contacts fournisseurs.
Communication	Préparer un message d'attente (« holding statement ») validé par la direction.
	Tenir un carnet d'événements horodaté pour les notifications (CNIL ≤ 72 h).
Amélioration continue	Réviser trimestriellement seuils et critères après chaque incident.
	Tester par un exercice sur un des scénarios cyber au minimum une fois par an.

< Campus Cyber >

< Juin 2026 >