ADN 49

Attaques Cyber : c’est arrivé près de chez vous

>> Angers - 23/02/2022

@adnouest

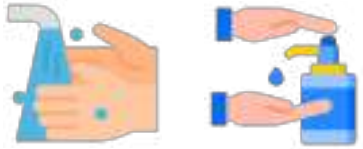
Marina Mendoza

ADN Ouest

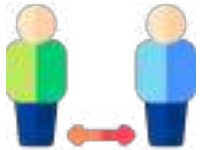
Chargée d'animation réseau et communication

N’oublions pas ces quelques précautions sanitaires

Restons **masqués** et pensons à garder le masque assis et lors des déplacements



Pensons à nous **laver et à nous désinfecter** les mains régulièrement



Veillons à rester à **1 mètre de distance** des autres participants

Si nous nous sentons **fiévreux ou malade**, rentrons chez nous pour ne pas (faire) prendre de risque

ADN Ouest : Agir pour le Développement du Numérique en Pays de la Loire et en Bretagne

UN LARGE RÉSEAU

+640 Structures adhérentes

+3700 Membres

100 Évènements

2 Régions

4 ENJEUX MAJEURS

- Emploi et formation
- Transition Numérique
- RSE
- Innovation

7 COMMUNAUTÉS THÉMATIQUES

- Numérique Responsable
- Santé
- Infra & services
- Cybersécurité
- Stratégie Digitale
- Data
- Management

DES PROGRAMMES AU SERVICE DE LA FILIÈRE

- 2 Observatoires : métiers et compétences numériques / économie et investissements
- 1 Fonds de Dotation : ADN Solidarity
- 1 accélérateur de projets innovants : ADN Booster

DES PÔLES TERRITORIAUX

ADN 44
ADN 29
ADN 49
ADN 56
ADN 35
ADN 22
ADN 85

DES CERCLES METIERS

- DPO
- DSI
- CMO

Franz Jarry

ADN Ouest

Directeur Général

Christophe Rouvrais

ESAIP

Directeur Général

Déroulé

18h00 : accueil des participants

18h10 : Introduction de l'état de la menace cyber par Franz Jarry, DG d'ADN Ouest

18h20 : Retour d'expérience d'Angers Loire Métropole par Constance Nebbula

18h40: Retour d'expérience de la Clinique de l'Anjou par Florent Delaruelle

19h00 : Se mettre dans la peau d'un hacker par Karim Zkik

19h20 : Questions-réponses

19h40 : Présentation de la communauté CyberFox

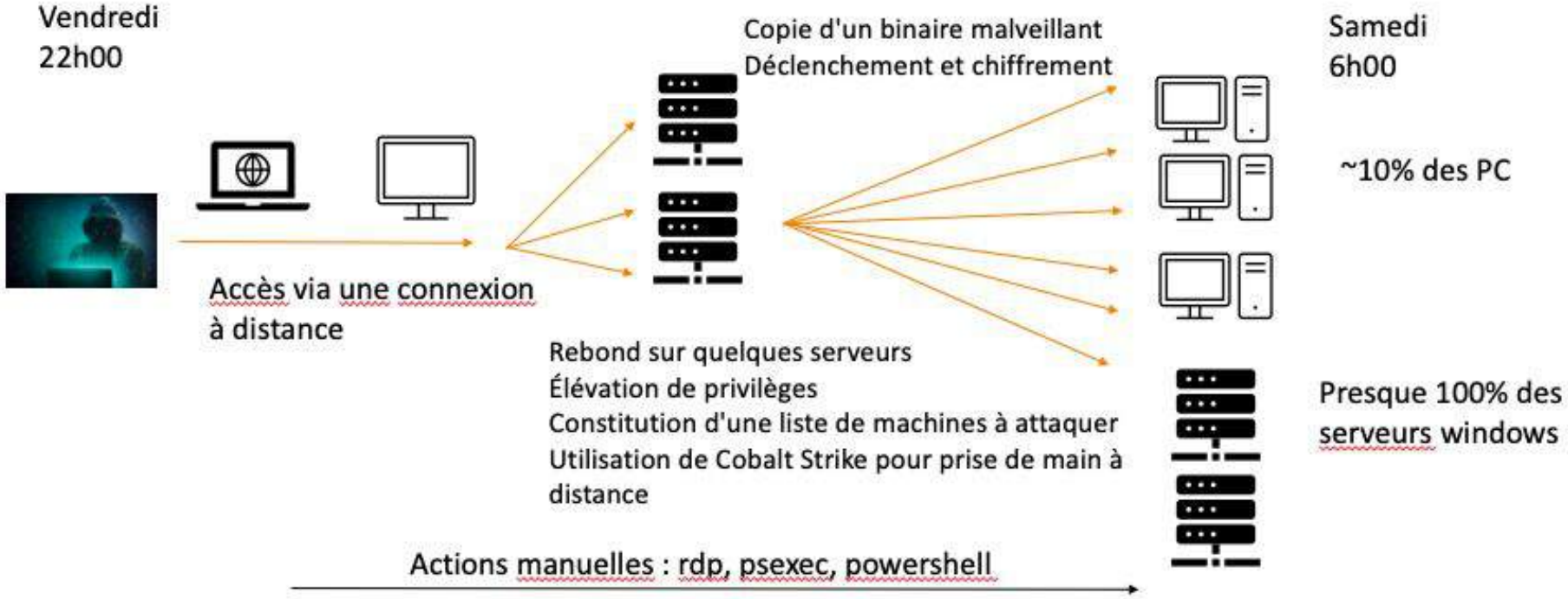
19h45 : poursuites des échanges librement

Constance Nebbula

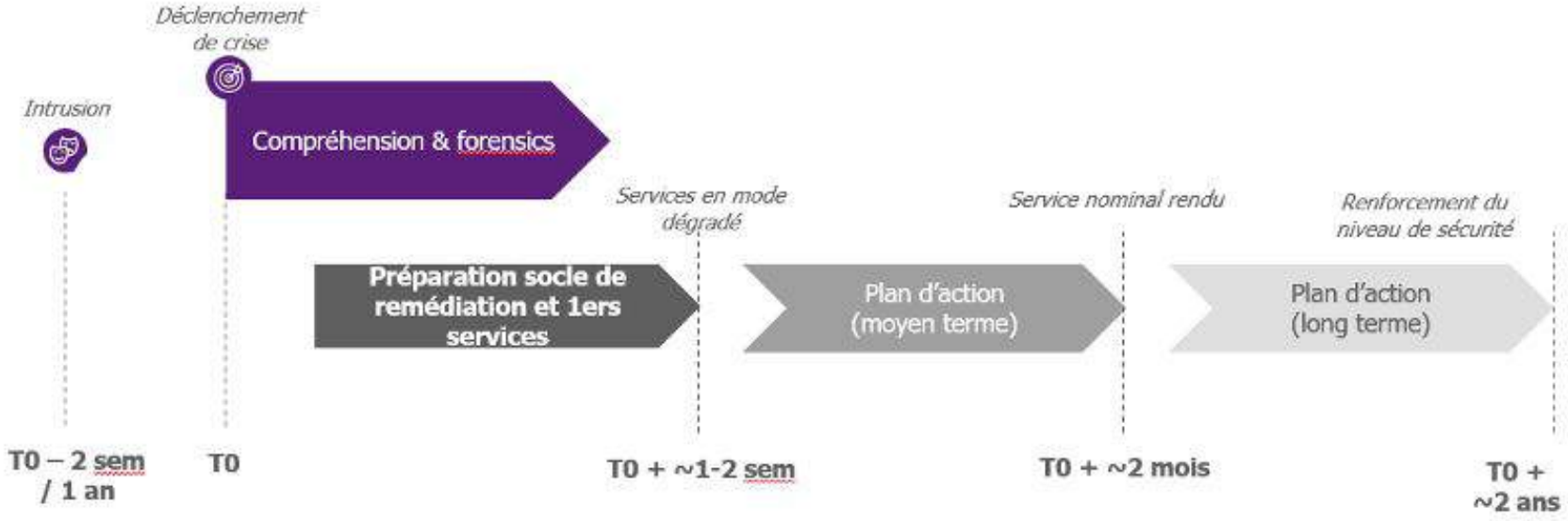
Elue de la ville d'Angers et d'Angers Loire Métropole

Déléguée à la transition numérique et au territoire intelligent

Le schéma de la Cyberattaque



La démarche envisagée



5 chantiers DSI pour gérer la situation

1 Active Directory

2 Réseau

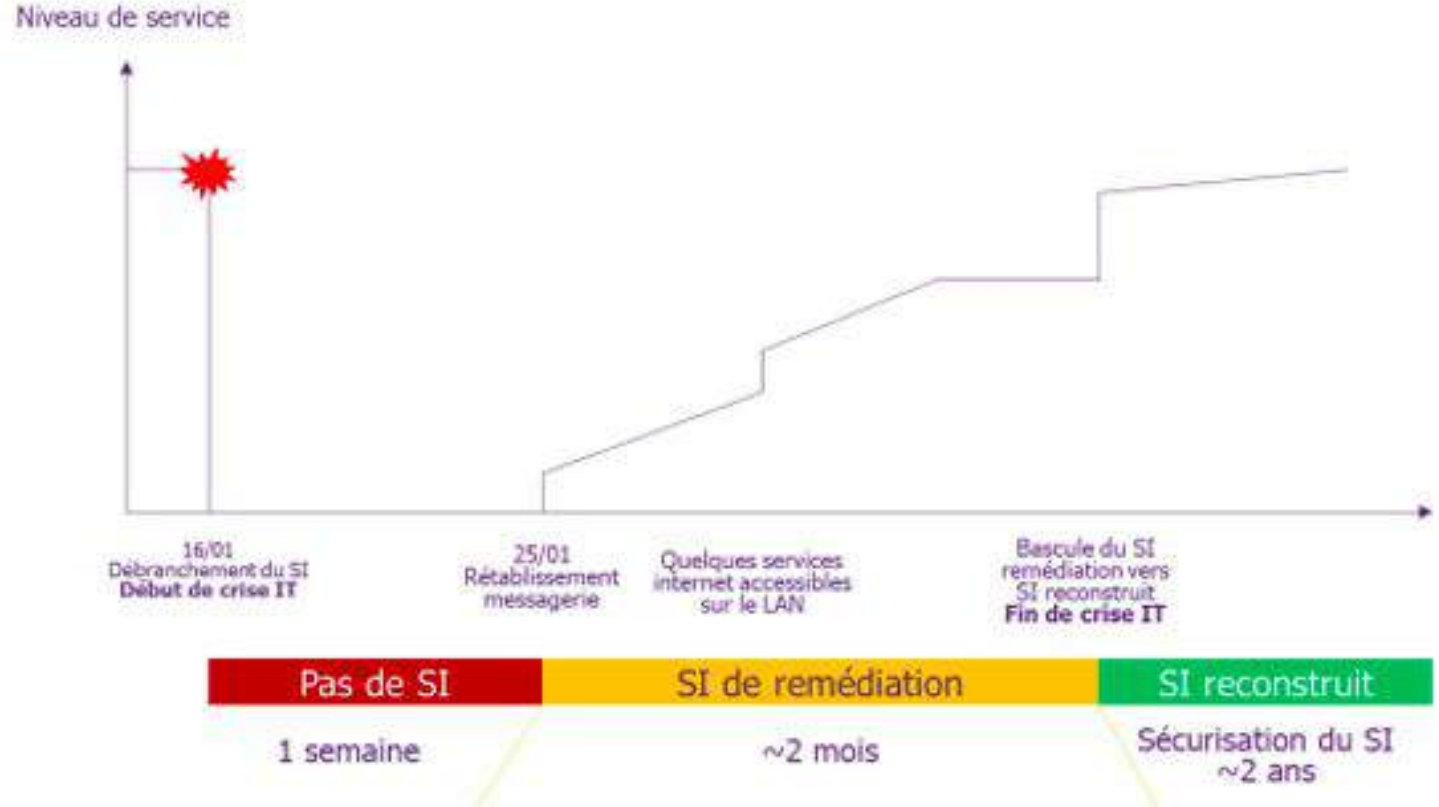
3 Recovery serveurs/ applis

4 Recovery Poste de travail

5 Forensics / monitoring

La cyber-attaque

La démarche envisagée



RECONSTRUCTION DU SI

Feuille de route globale pour la reconstruction du SI

Florent Delaruelle

Clinique de l’Anjou

DSI

CLINIQUE DE L'ANJOU

CLINIQUE DE L'ANJOU

CYBERATTAQUE - REX

Samedi 23 janvier 2021

- Contexte
- Processus de la Cyberattaque
- Chronologie Organisationnelle
- Cellule de crise
- Plan d'action et Plan de reconstruction
- Architecture Avant / Après
- Investissement Humain & Coût Financier
- Rapport Expert Cyber
- 1 an après
- Conclusion

Contexte

CLINIQUE DE L'ANJOU

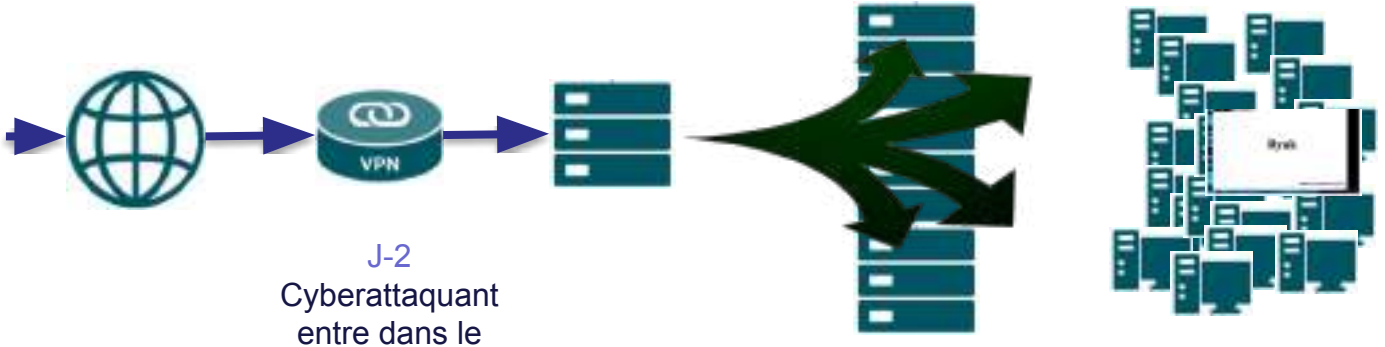
- La Clinique de l'Anjou
  - MCO – Urgence – Maternité Niv2
  - 380 lits - 650 salariés CDI – 160 médecins
  - 21 salles de bloc + 6 salles d'accouchement + 5 salles Soins Externes & IVT
  - 1 Robot chirurgical Da Vinci – Stérilisation interne – PUI – Cuisine interne
  - 80 000 séjours par an.
  - CA : 53 M€

- Les Systèmes d'information
  - Généralisation de l'informatisation des services en 2010 (Services de Soins, Blocs, Stér, Pharmacie, Urgences, Maternité, Cuisines, Services administratifs, Archives…)
  - Liens informatiques directs avec la Radiologie, le Laboratoire, les Cabinets des médecins qui sont sur le site, le CSSR.
  - +400 postes informatiques et +70 serveurs – 25 logiciels principaux.
  - Biomédical en partie informatisé (Per-OP, Monitoring Maternité, GMAO…)
  - Téléphonie en partie virtualisée

- Projets informatiques en cours avant l'attaque
  - Migration du DPI Emed vers le DPI Expert Santé en cours de démarrage
  - Externalisation de l'hébergement des logiciels cœur de métier (DPI/GAP)

Processus de la Cyberattaque

J-XX
Cyberattaquant déjà entré dans le SI à une date inconnue.



L'opération provient de l' étranger et est passée par les Pays-Bas

J-2
Cyberattaquant entre dans le S.I. via une vulnérabilité du portail d'accès extérieur ou un login/mot de passe. (identification des premières traces)

J-1 Prise de possession des premiers serveurs téléchargement des charges malveillantes (type CobaltStrike)

Samedi 23/01 2h30
Lancement de l'attaque :
- Elévation de privilèges
- Lancement du chiffrement
- Pratiquement tous les serveurs et postes infectés en quelques heures (3 à 4h)

Chronologie Organisationnelle

CLINIQUE DE L'ANJOU

Samedi 23/01 : Cyberattaque

- 2h30 Début de l'attaque
  Cryptage des fichiers
- 4h Appel support car DPI indisponible : Analyse du support
- 5h Déclenchement du Mode dégradé : impressions de secours
- Constat : pratiquement tout est crypté.
- 8h20 Appel DSI
- 8h25 Appel DG
- 8h30 Rappel des techniciens info

- **Difficultés :** Communications, liste des numéros, plus de mail…

Samedi 23/01 Actions très court terme

- **Actions ORGANISATIONELLES**
- 9h Mode dégradé :
  -Urgences / Admissions : papier
  -DPI : papier
- Premières actions d'urgences
- Création adresses Gmail
- Rappel des cadres

- **11h45 Cellule de crise**
  -Point de situation et actions :
  -Communication (Affichage, appels…)
  -Rappel des médecins selon besoins
  -Alerte Régulation, ARS, garde CHU
  -Alerte ANSSI, CNIL
  -Déposer plainte à la PJ (26/01)
  -Alerte Prestataires / Editeurs logiciels
  …
- 20h30 Prestataire Assurance Cyber
  Inquest / IntraSec / Databack

- **Actions TECHNIQUES**
- 10h Aviti : support système
- 10h Déconnexion des liens externes et des matériels du réseau interne
- 14h Illico Réseau support réseau
- 16h45 : ARS Auriane Lemesle
- 17h Point ANSSI – CERT-fr

- Sauvegardes sur bandes semblent OK
- Téléphonie fonctionnelle

Dimanche 23/01 : Organiser la semaine

- **Actions ORGANISATIONELLES**
- Communication affichage interne « ne pas allumer les PC »
- Etat des lieux Informatique et de la PEC patient (Appro & stock médicaments / DMI…)

- **Premières décisions**
- Accélérer la Migration du DPI sur ExS
  -Admissions
  -Stocks
  -Bloc
  -Soins / Prescriptions
  -Flux(Labo/Radio…)

- **Actions TECHNIQUES**
- Bloquer Internet et ouvrir en liste blanche
- Imprimantes en USB
- PC : réinstallation en W10
  - Accès à ExS Gestion des lits

Chronologie Jours suivants

CLINIQUE DE L'ANJOU

Lundi 25/01 : J+2

•Maintien de l'activité

•Retard sans conséquence sur le programme opératoire
•Mode dégradé papier
•Programme opératoire complet car imprimé 1 semaine à l'avance

•Accès au DPI ExS sur quelques PC (Gestion patient / Gestion des lits / Admission)

•A distance ANSSI/INQUEST-INTRASEQ
-Plan d'actions Forensic
-Analyse des serveurs et quelques postes
-Sortir les journaux du parefeu
-Mettre un EDR ?

•TECHNIQUE

•25/01 envoi des bandes pour restauration rapide par Databack

•Présence des prestataires locaux :
-Récupération et formatage PC
-Situation serveurs
-Gestion réseau

Jours suivants

••Choix du plan d'action :

••refaire le réseau (VLAN) pour plus segmenter le réseau
••Nouvelle infra systèmes (Windows 2019 au lieu de 2008 et 2012)

••Recensement et priorisation des besoins.

••RH :
-Paie des salariés : rejouer paie de décembre (à 3 jours des versements des salaires)
-Gestion des plannings du personnel (impression existante / appels)

••Quid de la rançon ? □ Ne pas payer / pas de prise de contact □ confié aux services compétents (PJ)

••SFR : augmenter la bande passante (MàJ des postes et accès DPI) □ Changement de prestataire pour Orange

Semaines / Mois suivants

••Remise en marche progressive du SI

••Arbitrage des priorités

••Améliorer la sécurité

••Reprendre les projets

Cellule de crise

- La mise en place dès le matin de la cellule de crise
  - Prise en compte de l'ampleur de la situation
  - Mise en place des actions pour continuer la PEC patients
  - Alerter les organismes (Labo/radio, ARS, ANSSI, Régulations…)
  - Préparer la Communication interne et externe
  - Priorisation de remise en place des logiciels et matériels

- La principale question du WE était de savoir si la Clinique était en capacité, sans son SIH, à fonctionner normalement et maintenir le programme de la semaine à venir ???
  - Mode dégradé
  - Utilisation du nouveau DPI pour les admissions
  - Planning opératoire S+1 imprimé
  - Stock pharmacie

  - opérationnel
  - remise en marche PC admissions
  - Planning prêt
  - Pas d'état gestion au quotidien

Plan d'action

CLINIQUE DE L'ANJOU

Plan d'Action

- Déconnecter
  - Les éléments du réseau
  - Les liens externes
- Alerter
  - Interne / Externe
  - ANS, CNIL, ARS
  - Dépôt de plainte
- Ne pas payer la rançon
- Investiguer / Identifier / Remédier
  - Où ? Comment ?
  - Exfiltration de données ?
  - Corriger les failles
  - Bloquer les canaux utilisés
  - Restaurer plan de reconstruction

PLAN D'ACTION

Administratif

- ✓ Alerte ANSSI
- ✓ Alerte CERT-FR
- ✓ Alerte ARS
- ✓ Alerte CNIL
- ✓ Porter plainte
- ✓ Main courante
- ✓ Tenir un listing des actes

RESEAU

- ✓ Couper accès internet mise en place liste blanche (Expert santé…)
- ✓ Modifier mot de passe Wifi ANJOU (dans que les postes se connectent)
- ✓ Voir si laisser wifi nomade / Médecins → reste actif que accès à internet
- ✓ Bloquer les règles permettant les accès inter-VLAN avec l'ancien réseau contaminé
- ✓ Enlever toutes les machines du réseau + mettre étiquette ne pas utiliser
- ✓ Activer le proxy sur le Firewall pour voir les accès internet
- ✓ Scanner le réseau pour vérifier qu'il n'y a plus de postes
- ☐ Voir avec SFR pour augmenter la bande passante (téléchargement des Maj Win)

SERVEURS

- ✓ Déconnecter tous les serveurs du réseau
  - ✓ Serveurs téléphonie en fonction
  - ✓ Serveurs Mailer en fonction
  - ✓ Serveur Télécare santé en fonction
  - ✓ Serveur Appel Malade
- ✓ Analyser le DC avec outils CERT-FR → en cours mais Serveur bloqué → Analyse des disques
- ✓ Analyser les serveurs avec outils intrusion → fait pour Ernest-SQL+HYVSQH2PC
- ✓ Prélever prestataires pour RH
- ✓ Plan de reconstruction

PC

- ✓ Déconnecter tous les postes du réseau
- ✓ Portables : Récupérer, formater, +WLAN pour accès opi / letto / ambulo (mode dégradé)
- ✓ PC Fixe : plan de reconstruction

APPLICATIFS

- ✓ Démarrage EpS Annuaire
- ✓ Démarrage EpS OS Anaxih
- ✓ Démarrage EpS GDL
- ✓ Démarrage EpS Stock → Jeudi 28/01 - Rémi Blanchais sur place le 02/02
- ✓ Démarrage EpS Bloc / DMI → En cours
- ✓ GIDEMS PMSI / FACTURATION → GDS à transférer chez Berger Levrault Attente Réseau
- ✓ Attente retour DATABACK → récupération possible - prévoir les ressources → Envoyé à INTRINSEC

→ VOIR LISTE DES SERVEURS plus bas

Plan de reconstruction

CLINIQUE DE L'ANJOU

Plan de Reconstruction

- Nouveau Réseau
- Nouveau Socle Systèmes
- PC formatés ou nouveaux
- Sécurité +

PLAN DE RECONSTRUCTION

RESEAU

- Définition de la nouvelle typologie réseau
- Création des VLAN au niveau du pare-feu
- Déploiement des VLAN sur les consoles des Switches
- Mise en place des VLAN pour les VLAN
- Déploiement des VLAN sur chaque poste des services
  - Prévoir une ressource pour aider Thomas → Bastien / Mathieu
  - Prioriser les secteurs :
    - Bloc
    - FACTURATION / PMSI
    - BLOC
    - STER
    - PHARMA
    - DIRECTION
    - COMPTA
- Thomas / Mathieu prévoir un tableau de suivi
- Réinventorier des liens entre l'existant
  - Tweetgrey
  - Radiologie
  - CS3/KR / Pleasco vert
  - Liens IFlux
    - SQS
    - Sagetis

SERVEURS

- Création Nouvel HYPERVISEUR W2016 Datacenter sur serveur physique existant
- Création Nouvel AD W2016 → en virtuel + bascule serveur physique
- Monter des VM vierges pour les applicatifs → voir liste dans rubrique APPLICATIFS
- Achat d'un nouvel Hyperviseur en Mai 2016 Data Center
- Création ferme RDS sur W2016 → devis licences RDS 2016
  - Office 2013 compatible sur Windows Server 2016 → à tester
  - Ne pas utiliser l'UPD pour pouvoir utiliser le multisession
- Booster le temps et Prévoir ressource pour continuer les actions serveurs (VEEAM (Durs appli) (+6) au 02/02)
- Prévoir un onduleur
- Remonter la solution de sauvegarde → retour du serveur 01/02 fin de journée
  - Refaire les jobs de sauvegardes ! pour info
  - Prévoir bandes LTO pour sauvegarde sur bandes

PC

- Prévoir un tableau de suivi
- Mise en place du serveur PDS pour limiter la bande passante
- PC Nuxo : récupérer, formater, Win 10, Maj, Prioriser → Yanying / Mathieu / Nathan / Axel
- Formater les PC
- compte local admin avec mot de passe différent sur chaque poste peut se faire après : LAPS sur AD
- Coller une pastille 2021 / 02 pour repérage des PC réinstallés
- Réintégrer les PC dans le domaine
- Installation des applications particulières par GPO (Office, ...)
- Prévoir remplacement des Clients Légers & PC Obsolètes +115 postes

INFRASTRUCTURE SYSTEME

- Création AD du domaine "clinique-anjou.fr" 2j
  - Architecture en 3 tiers
  - Création des comptes utilisateurs → utilisateur.clinique.com
    - pas d'utilisateur "Admin" / ni en local
  - Utilisation AppLocker
  - Création des stratégies de groupes
    - Déploiement des raccourcis
    - Déploiement des imprimantes
- Création du DHCP avec réservation 1/2J
- Création VM Antivirus + GPO 1h
- Création serveur de sauvegarde + JOB 1/2J
- Création VM Exchange ? 1,5J certificat?
- master2016
- Création serveur d'impression + GPO 1J
- Création Serveur de fichiers 1h + refaire les répertoires et droits d'accès
- Création VM ferme RDS 2016 + Office 2013 3J
  - serveur dédié Fiennes / Broker / HPD (ajout2013)
- Création VM WSUS 2h GPO
- Création VM applicatifs 1h par VM
- → VOIR LISTE DES SERVEURS plus bas

SECURITE

- Route Essentiels
- Fonctionne sur nouvel infra ?
- Anti-virus
- EDR
- Séparation des réseaux
- Collecteur de Log
- Surveillance AD
- CRADAD sur AD
- SAUVEGARDE
- Sensibilisation du personnel
- Fonctionnalité de gestion des extensions fichiers (APPGHDKTA)

DIVERS

- TPE
- Serveur RDS ou client lourd ?

Architecture avant / après

Domaine	AVANT	APRES
Portail d'accès	1 seul login : utilisateur/mot de passe	Utilisateur / mot de passe + authenticator Pas d'accès direct aux serveurs (rebond RDP)
Réseau	1 VLAN clinique et quelques VLAN biomed / cabinets / téléphonie	Segmentation plus forte VLAN soins / administratif / serveur etc…
Serveurs	Windows 2008/2012 Administrateur du domaine MàJ ponctuelles	Windows 2016/2019 Séparation 3 tiers (t0/t1/t2) & Silot MàJ mensuelles Règles d'accès renforcées
PC	Windows 7 / 10 MàJ ponctuelles Utilisateurs Admin Local Clients légers XP/W7e	Windows 10 MàJ très régulières Utilisation de LAPS (admin local renforcé)
Mot de passe	Génériques dans les service avec mot de passe = identifiant	Politique de Mots de passe complexe pour tous les comptes
Sensibilisation	Par mail régulièrement	Plus active / Quizz / tests de phishing / formation

Renforcement de la sécurité : plus de règles au niveau du parefeu, GéoIP, gestion plus réglementée des machines non gérées, plus de restrictions utilisateurs…

Investissement Humain & Coûts

- Investissement humain très important
  - Présence tout le WE « sans horaire »
  - Mobilisation très forte de l'encadrement
  - Il faut tenir dans la longueur
  - Attitude compréhensive du corps médical
- Gestion des coûts
  - Renouvellement de 30% des PC
  - Coût de réinstallation de la plupart des éditeurs logiciels
  - Coût élevé de l'expertise (Assureur)
- Gestion Financière
  - Maîtrise difficile car aucune visibilité
  - Avance de la CPAM / Crédit court
  - La non-déprogrammation à limité les pertes financières

COÛT TOTAL : 400K€

Prise en charge assurance estimée à 150K€

CLINIQUE DE L'ANJOU

Rapport Expert Cyber

Extrait du rapport de Réponse à Incident

- Les investigations menées permettent d'assurer avec un niveau de confiance élevé, la **compromission totale** du système d'information de la Clinique de l'Anjou, par l'acteur malveillant **Ryuk**.
- L'acteur malveillant Ryuk est opportuniste et ses objectifs sont purement financiers.

- Les analyses effectuées permettent d'identifier les premières traces de l'adversaire le 21 janvier 2021 à 21h42 à partir de connexions depuis l'adresse IP XX.XX.XX.XX vers le serveur VPN SonicWall exposé sur Internet.
- Aucun élément n'a permis d'identifier le vecteur d'intrusion utilisé par l'adversaire. Cependant d'après les éléments observés les hypothèses les plus probables sont :
  - L'obtention d'un couple login/mot de passe valide par l'acteur malveillant permettant de se connecter au VPN
  - **L'exploitation de la vulnérabilité** CVE-2021-20016. Il est à noter que cette vulnérabilité a été publiée le 23 janvier 2021 et le correctif était disponible le 3 février 2021, il n'était donc pas possible pour la Clinique de prévenir l'exploitation du 21 janvier.

- Quelques déplacements dans le système d'informations ont été observés peu de temps après, notamment via le protocole Remote Desktop Protocole.
  L'adversaire a ensuite scanné le système d'information de la Clinique d'Anjou et s'est propagé latéralement, il a téléchargé des charges malveillantes (possiblement CobaltStrike) sur plusieurs serveurs.

- Finalement, l'adversaire a lancé le chiffrement du système d'information depuis, au moins, deux serveurs. Les premières **traces de chiffrements par le rançongiciel Ryuk ont été identifiés à partir du 23 janvier** 2021 à 02h31 sur le contrôleur de domaine.

- Les analyses des journaux du pare-feu n'ont pas révélé de trace d'exfiltration de données de la part de l'adversaire.

1 an après…

- L'ensemble de l'activité informatique a été remis en fonctionnement
- Des fonctions non-essentielles sont à finaliser :
  - Accès sur les Smartphones de la messagerie
  - Récupération de données de certains logiciels abandonnés
  - 2 Logiciels Service BioMédical « non-essentiels »
  - Serveurs de TEST
  - Scan to mail et Scan to Folder des Copieurs (partiel) (Sécurité)

- …Rattraper le retard pris sur les projets (HOP'EN, portail patient, CDRi, archivage…)
- Validation des modes dégradés des logiciels hébergés à l'extérieur depuis la cyberattaque.

- De nouveaux projets liés à l'attaque
  - Continuer d'augmenter la sécurité *(veille technique)*
  - Formation des utilisateurs à la Cyber-sécurité *(fait et à renouveler)*
  - Tests d'intrusion *(fait et à renouveler)*
  - Copie locale des hébergements extérieurs *(PCA)*

Conclusion

- Forces
  - Mobilisation forte des cadres
  - Modes Dégradés Fonctionnels
  - Prestataires locaux réactifs
  - SI local : connaissance du contexte
  - Compréhension des différents acteurs
  - Soutien de la CPAM pour la Trésorerie
- Faiblesses
  - Détection tardive de l'attaque
  - Accompagnement hors site
  - Temps de remise en œuvre
  - Retard dans la Facturation
  - Trésorerie des médecins
- Débats & Combats

Remise à niveau du SI ou restauration à l'identique ?
Redémarrage sur les logiciels existant ou accélération du nouveau DPI ?
Abandon du projet pilote certification HAS V2020 et retour à la date initiale septembre 2023

CLINIQUE
DE L'ANJOU

Karim Zkik

ESAIP

Enseignant-chercheur

C’est arrivé près de chez vous

Attaques cyber: Challenges, Défis et Solutions

PRÉPARÉ PAR:

- ZKIK KARIM

23 février 2022

Introduction

A DEFINITION OF CYBER SECURITY

La cybersécurité fait référence à l'ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les appareils, les programmes et les données contre les attaques, les dommages ou les accès non autorisés.

La cybersécurité peut également être appelée sécurité des technologies de l'information.

Introduction

Pourquoi la cybersécurité est-elle importante ?

1- Connexion 24h/24 et 7j/7

2- Augmentation de la cybercriminalité

3- Impact sur les entreprises et les particuliers

4- Législation et responsabilités

5- Prolifération des menaces

6- La sophistication des menaces

Introduction

Impact de la cybercriminalité sur les entreprises :

1- Baisse de la productivité

2- Perte de chiffre d'affaires

3- Publication de données sensibles non autorisées

4- Menace des secrets commerciaux des formules

5- Compromis de réputation et de confiance

6- Perte de communication

7- Menace sur les systèmes environnementaux et de sécurité

8- Perte de temps

Exemples d'attaques

2020 : Marriott

- Pour la deuxième fois en deux ans, la chaîne d'hôtels populaire a subi une violation de données.
- Le 31 mars, Marriott a publié une déclaration révélant que les informations de 5,2 millions d'invités ont été consultées à l'aide des identifiants de connexion de deux employés d'un établissement franchisé.
- Les informations compromises peuvent avoir impliqué des coordonnées et des informations relatives aux comptes de fidélité des clients, mais pas des mots de passe.

Exemples d'attaques

2020/2021 : Solarwinds/ FireEye

- FireEyea déclenché une chaîne d'événements le 8 décembre lorsqu'il a révélé que des pirates informatiques présumés d'un État-nation avaient violé le fournisseur de sécurité et obtenu les outils de l'équipe rouge de FireEye.

- Le 13 décembre, la société a révélé que l'attaque de l'État-nation était le résultat d'une attaque massive de la chaîne d'approvisionnement contre SolarWinds

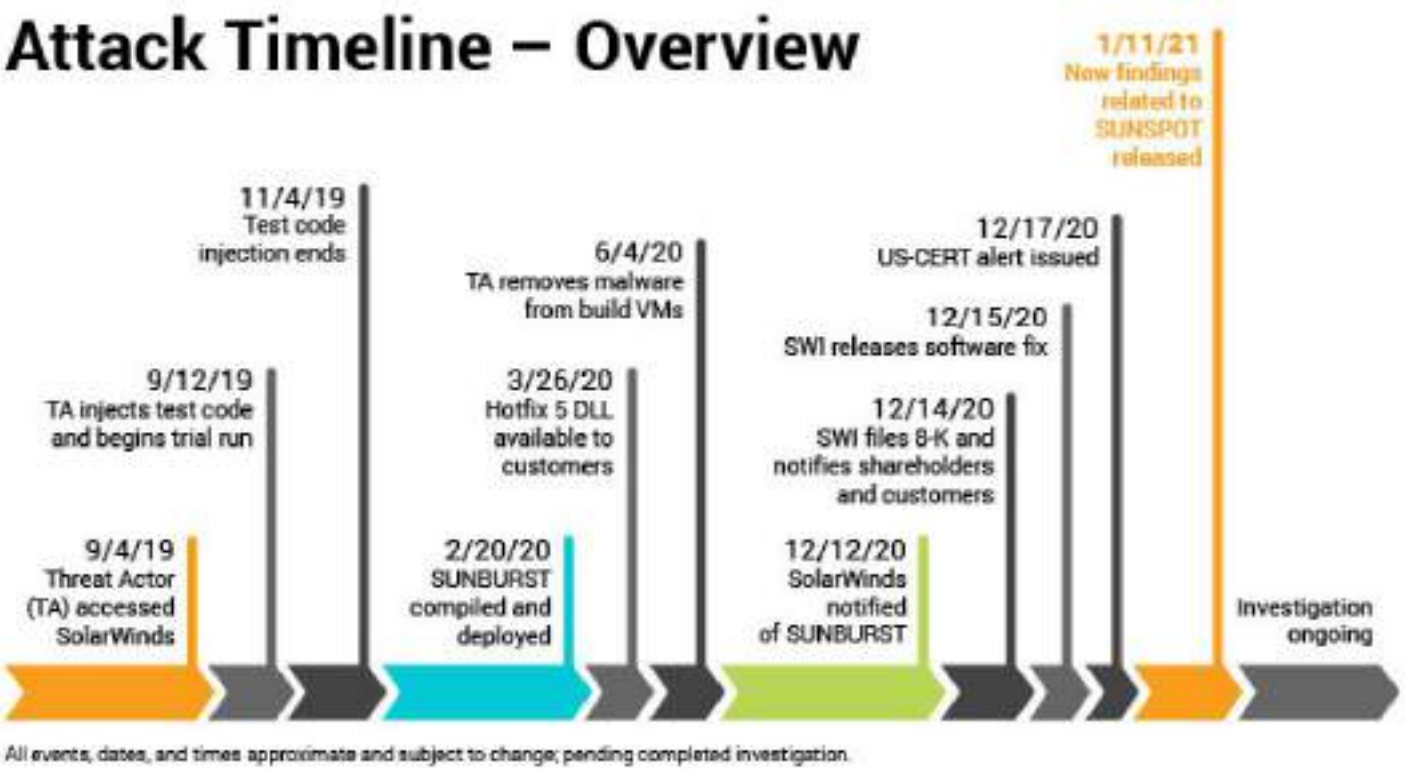
- Elle permettait aux acteurs malveillants d'accéder à de nombreux réseaux gouvernementaux et d'entreprises à travers le monde.

- Selon une déclaration conjointe du 17 décembre du FederalBureau of Investigation, de la Cybersecurityand Infrastructure Security Agency et du Bureau du directeur du renseignement national, les attaques se poursuivent.

- Depuis la déclaration, de grandes sociétés technologiques telles qu'Intel, Nvidiaet Cisco ont révélé avoir reçu les mises à jour malveillantes de SolarWinds, bien que les sociétés aient déclaré n'avoir trouvé aucune preuve que des acteurs malveillants aient exploité les portes dérobées et pénétré leurs réseaux.

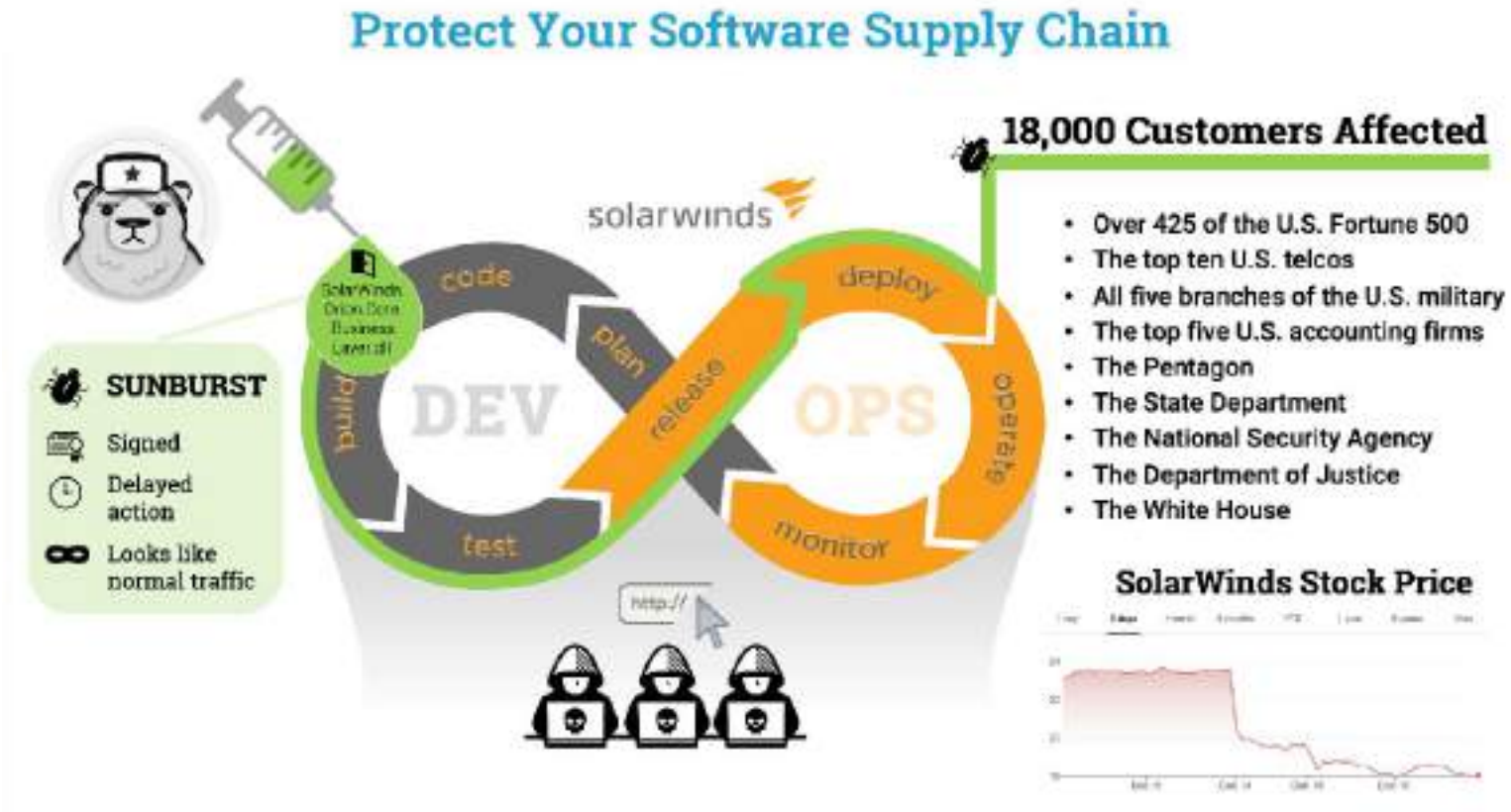
Exemples d'attaques

2020/2021 : Solarwinds/ FireEye



Exemples d'attaques

2020/2021 : Solarwinds/ FireEye



Exemples d'attaques

2022 : Ukrain vs Russia

- En Ukraine, une cyberattaque alimente les tensions avec Moscou.
- L'Ukraine a affirmé, dimanche, avoir des « preuves » de l'implication de la Russie dans la cyberattaque massive.
- L'Ukraine a affirmé, dimanche 16 janvier, avoir des *« preuves »* de l'implication de la Russie dans la cyberattaque massive qui a visé plusieurs sites gouvernementaux dans la nuit du 13 au 14 janvier. *« A ce jour, toutes les preuves indiquent que la Russie est derrière la cyberattaque »*, a déclaré le ministère de la transformation numérique, sans plus de précisions.
- le géant informatique américain Microsoft a toutefois averti, dimanche 16 janvier, que cette cyberattaque pourrait rendre toute la structure informatique du gouvernement ukrainien inopérable.

Exemples d'attaques

Les Attaques en 2021

Le premier semestre 2021 a vu 1,5 milliard d'attaques contre des appareils intelligents, avec des attaquants cherchant à voler des données, à exploiter des crypto-monnaies ou à créer des botnets.

Selon une analyse de Kaspersky de sa télémétrie à partir de honeypots partagés avec Threatpost, la société a détecté plus de 1,5 milliard d'attaques IoT, contre 639 millions au cours du semestre précédent, soit plus du double du volume.

	H2 2020	H1 2021
telnet	460,703,861	872,345,837
ssh	142,245,141	514,749,073
web	36,206,940	128,619,349

The number of total infection attempts broken down by type of honeypot

La cybersécurité relève de la sécurité nationale

- Le président Biden a convoqué une réunion à la Maison Blanche le mois d'octobre 2021 dernier pour se concentrer sur la cybersécurité.

- Après des mois d'escalade des cyberattaques qui ont affecté les fournisseurs d'infrastructures critiques, la chaîne d'approvisionnement alimentaire et même perturbé la distribution des vaccins COVID-19 et les hôpitaux à pleine capacité luttant pour traiter les patients COVID, il est temps de tirer un trait sur le sable.

- Une chose qui est de plus en plus évidente à mesure que les frontières se brouillent pour les cyberattaques, c'est que la cybersécurité est la sécurité nationale.

Les défis de la cybersécurité

Challenges of cybersecurity

- Sécurité du réseau
- Sécurité des applications
- Sécurité des terminaux
- Sécurité des données
- Gestion des identités
- Sécurité des bases de données et des infrastructures
- Sécurité cloud
- Sécurité mobile
- Planification de la reprise après sinistre/de la continuité des activités

Les défis de la cybersécurité

Preventing insider threats

Risques Interne: Risque de compromission interne

La menace interne est le risque que des employés, des sous-traitants et d'autres initiés, actuels et anciens, exploitent leur accès privilégié aux systèmes pour voler des informations ou de l'argent, ou causer des dommages à l'organisation.

Les attaques les plus coûteuses et les plus dangereuses sont souvent perpétrées par des personnes de confiance

51 % des failles de sécurité des organisations ont subi une attaque interne

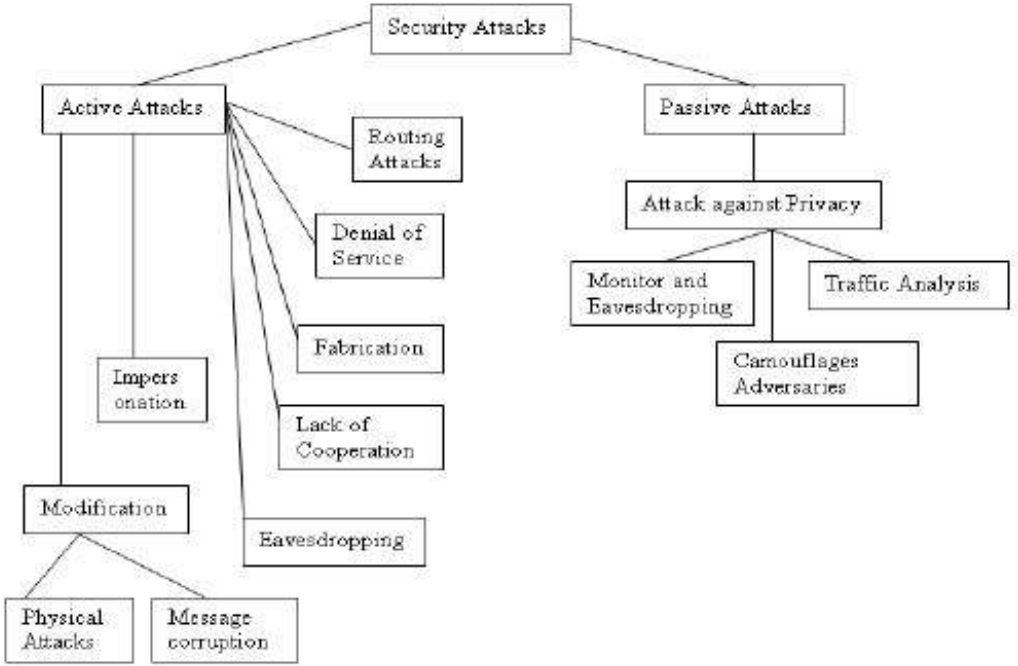
67 % des violations internes étaient plus coûteuses que les attaques externes

Les défis de la cybersécurité

Principales attaques :

Principales attaques courantes :

- ARP attack
- Brute Force Attack
- Malwares
- Flooding
- Sniffers
- Spoofing
- Redirected Attacks
- Tunneling Attack

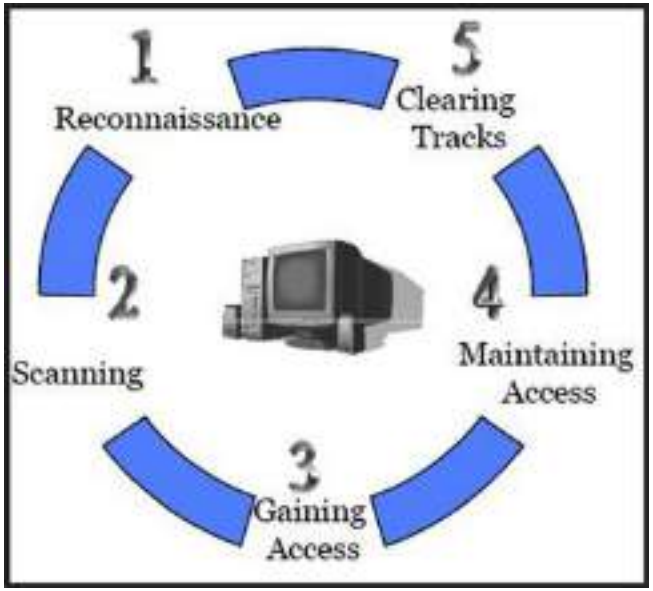


Les étapes d'une attaque

Les étapes d'une attaque

Cycle de vie de l'attaque :

- Reconnaissance
- Scanning (adresses, port, vulnerabilities)
- Gaining Access
- Maintaining Access
- Clearing Tracks



Gaining Access

Les phases précédentes du piratage, y compris l'empreinte et la reconnaissance, l'analyse, l'énumération et l'évaluation des vulnérabilités, aident les attaquants à identifier les failles de sécurité et les vulnérabilités qui existent dans les ressources informatiques organisationnelles cibles.

Les attaquants utilisent ces informations, ainsi que des techniques telles que le craquage de mots de passe et l'exploitation de vulnérabilités telles que les débordements de mémoire tampon, pour accéder au système organisationnel cible.

Privilege Escalation

Type of Escalation privilege

L'escalade des privilèges est requise lorsque vous souhaitez accéder aux ressources système auxquelles vous n'êtes pas autorisé à accéder. L'escalade de privilèges prend deux formes : l'escalade de privilèges verticale et l'escalade de privilèges horizontale.

Horizontal Privilege Escalation: Dans une élévation horizontale des privilèges, l'utilisateur non autorisé tente d'accéder aux ressources, fonctions et autres privilèges appartenant à un utilisateur autorisé disposant d'autorisations d'accès similaires. Par exemple, l'utilisateur bancaire en ligne A peut facilement accéder au compte bancaire de l'utilisateur B.

Vertical Privilege Escalation: Dans une élévation verticale des privilèges, l'utilisateur non autorisé tente d'accéder aux ressources et aux fonctions d'un utilisateur disposant de privilèges plus élevés, tels que les administrateurs d'application ou de site. Par exemple, une personne utilisant les services bancaires en ligne peut accéder au site en utilisant les fonctions d'administration.

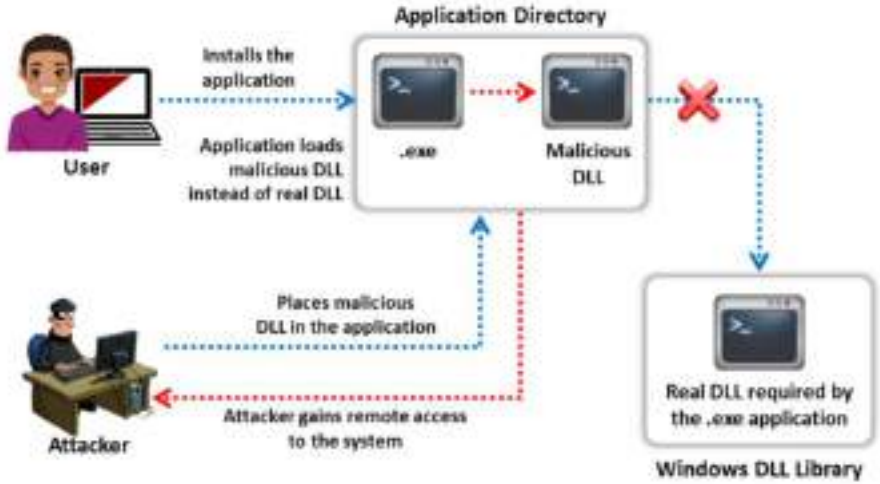
Privilege Escalation

Type of Escalation privilege

Privilege Escalation Using DLL Hijacking

La plupart des applications Windows n'utilisent pas le chemin complet lors du chargement d'une bibliothèque DLL externe ; au lieu de cela, ils recherchent d'abord le répertoire à partir duquel ils ont été chargés.

Prenant cela comme un avantage, si les attaquants peuvent placer une DLL malveillante dans le répertoire de l'application, l'application exécutera la DLL malveillante à la place de la vraie DLL.



Maintaining Access

Maintain Access

Une fois que les attaquants obtiennent des privilèges plus élevés dans le système cible en essayant diverses tentatives d'élévation de privilèges, ils peuvent tenter d'exécuter une application malveillante en exploitant une vulnérabilité pour exécuter du code arbitraire.
En exécutant des applications malveillantes, l'attaquant peut voler des informations personnelles, obtenir un accès non autorisé aux ressources système, cracker des mots de passe, capturer des captures d'écran, installer une porte dérobée pour maintenir un accès facile, etc.

Les programmes malveillants que les attaquants exécutent sur les systèmes cibles peuvent être :

- **Backdoors:** Programme conçu pour refuser ou perturber l'opération, recueillir des informations qui conduisent à l'exploitation ou à la perte de confidentialité, ou obtenir un accès non autorisé aux ressources du système.
- **Crackers:** Composants de logiciels ou de programmes conçus pour déchiffrer un code ou des mots de passe.
- **Keyloggers:** Ceux-ci peuvent être matériels ou logiciels. Dans les deux cas, l'objectif est d'enregistrer chaque frappe effectuée sur le clavier de l'ordinateur.
- **Spyware:** Un logiciel espion peut capturer des captures d'écran et les envoyer à un emplacement spécifié défini par le pirate. À cette fin, les attaquants doivent maintenir l'accès aux ordinateurs des victimes. Après avoir extrait toutes les informations requises de l'ordinateur de la victime, l'attaquant installe plusieurs portes dérobées pour y accéder facilement à l'avenir.

Clearing Logs

Clearing Logs

- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection

Attacker uses the following techniques to cover tracks on the target system

1. **Disable Auditing:** Disables auditing features of the target system
2. **Clearing Logs:** Clear/delete the system log entries corresponding to his/her activities
3. **Manipulating Logs:** Manipulates logs in such a way that he/she will not be caught in legal actions

Threat intelligence

Threat intelligence

Threat intelligence se compose de l'ensemble des activités qu'une organisation entreprend pour se renseigner sur les changements dans le paysage des menaces de cybersécurité et intégrer des informations sur l'évolution des menaces dans ses opérations de cybersécurité.

Open-Source Intelligence: Utiliser les informations publiques La collecte d'informations à partir de sources publiques librement accessibles est connue sous le nom de renseignement open source. Voici quelques-unes des sources de renseignements open source les plus courantes :

- Security websites,
- Vulnerability databases,
- The general news media,
- Social media,
- Information published on the dark web,
- Public and private information sharing centers,
- Security research organizations.

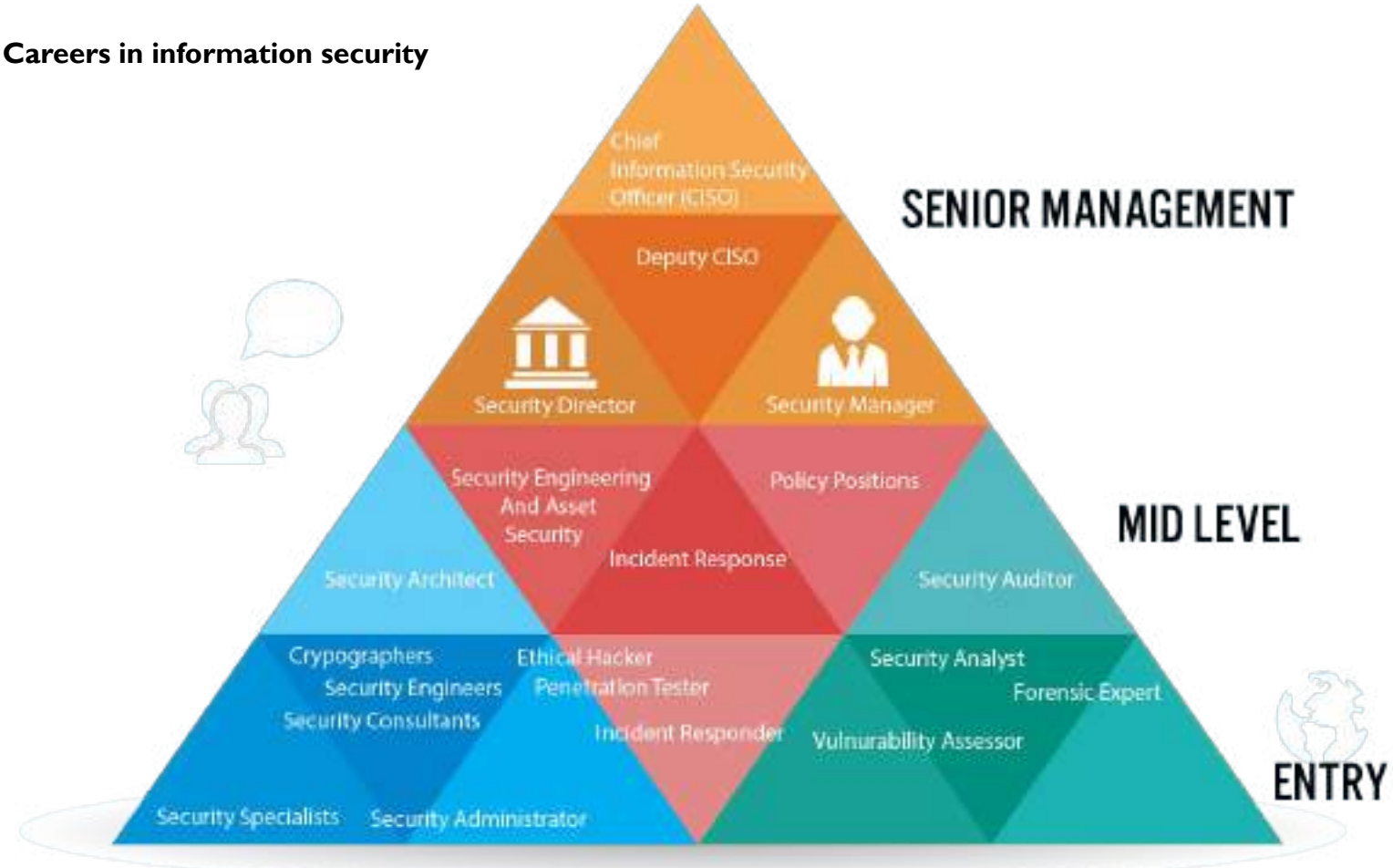
Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures ou CVE est un dictionnaire d'informations publiques sur les vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisation MITRE, soutenue par le Département de la sécurité intérieure des États-Unis.

https://www.cvedetails.com/

Security careers and opportunities

Careers in information security



Security careers and opportunities

Information security skills

Primary skills, with strong knowledge in:

- Coding ⇒ scripting and programing
- OS ⇒ Linux/Windows
- Network ⇒ OSI, TCP/IP, Services
- Databases
- Web

Advanced skills:

- Problem Solving
- System design
- Complex solution
- Troubleshooting /Debugging

Cybersecurity Market

Cyber security Market

Conclusion

“Cyber-Security is much more than a matter of IT.”.”

Stephane Nappo, VP CISO Groupe SEB (Ex CISO OVH et Société Générale)

Merci pour votre attention

Pour me contacter :

kzkik@esaip.org
karim.zkik@gmail.com

Site web:

https://karimzkik.com

Vous pouvez me retrouver aussi sur :

DBLP, Google Scholar, ResearchGate, ORCID et LinkedIn

Avez-vous des questions ?

Vos prochains événements ADN Ouest

24

[Visio] Cyber Meet #1 : venez échanger autour de l'analyse de risques

01

ADN infra&services : construisons ensemble les futurs projets de la communauté !

03

[Hybride] Libérée, délivrée... Comment la data gagne du terrain dans l'entreprise

17

[Hybride] Restitution enquête ORCN Bretagne & Pays de la Loire 2021

17

Afterwork ADN Vendée

21

Afterwork ADN Data

31

[Séminaire] Pourquoi et comment opérer une transformation digitale de votre entreprise ?

05

Intelligence artificielle et données dans l'industrie, quelles étapes pour atteindre vos objectifs ?

Votre avis compte !

Lien : klaxoon.com

Mot de passe : QZZTGNE

(un pseudo vous sera demandé)

Vous êtes au du numérique !

www.adnouest.org

Partagez votre expérience :
@adnouest