Cours ISO 27001

TP Blue vs Red Team - Correction

Etienne de Séréville, OCS IBM France, Relations Institutionnelles

Agenda

1. Consignes du travail dirigé

2. Etude de cas Société de Robotique (SR)

1. Consignes du travail dirigé

Equipes
- Blue Team: équipe de sécurité de la SR
- Red Team: représente des pirates externes

Objectifs
- Blue Team: cadrage de la planification du SMSI
- Red Team: créer un incident de sécurité induisant la réponse de l'équipe de sécurité de la SR

Timing – 3H
T0: Présentation des consignes de l'exercice et création des équipes
+10m - Prise en compte de l'énoncé et planification du SMSI
+1H – Présentation des plans
+2H – Organiser la réponse à l'incident et la cellule de crise
+2H20 – Présentation des réponses et de la cellule de crise
+3H Fin de l'exercice

Agenda

1. Consignes du travail dirigé
2. **Etude de cas Société de Robotique**

2. Etude de cas Société de Robotique (SR)

La Société de Robotique est une entreprise qui conçoit et fabrique des robots pour des usages civils et militaires sur mesure, comme Colossus pour les Pompiers, robot porteur, chariot filoguidé d'usine, etc.

Le siège de l'entreprise et le bureau d'étude sont situés en France. Les usines de fabrication sont en France et aux USA. Dix bureaux commerciaux sont à l'international. Le centre de téléopération est situé au siège.

Le personnel est composé de managers, de commerciaux, d'ingénieurs et de techniciens en robotique, du personnel administratif et d'informaticiens pour les besoins propres de l'entreprise.

Les 2 usines hébergent chacune un centre informatique, et chaque bureau commercial est équipé d'un local technique pour les serveurs et les équipements réseau de proximité.

Les équipements numériques se composent :

- Des applications informatiques pour la conception des robots (C&DAO, MAO…) sur serveurs d'application
- Des machines spéciales et des automates programmables pour les usines de fabrication (usinage, fraisage, câblage…);
- Des bases de données métiers (composants électroniques, mécaniques…) et certains logiciels (brevets…) sont en Saas;
- De logiciels pour la gestion administrative de l'entreprise (ERP, CRM, comptabilité, bureautique, messagerie);
- De logiciels d'infrastructures (routeurs, bornes Wifi, annuaire, serveurs de fichiers, d'impression, sauvegardes…);
- Et matériels utilisateurs: portable, tablette, smartphone, imprimante.

Les logiciels et applications sont achetés sur le marché, les développements informatiques sont limités à ceux embarqués dans les robots et le scripting de production.

Un prestataire informatique assure la maintenance informatique à distance et sur site en France lorsque nécessaire (changement de composants).

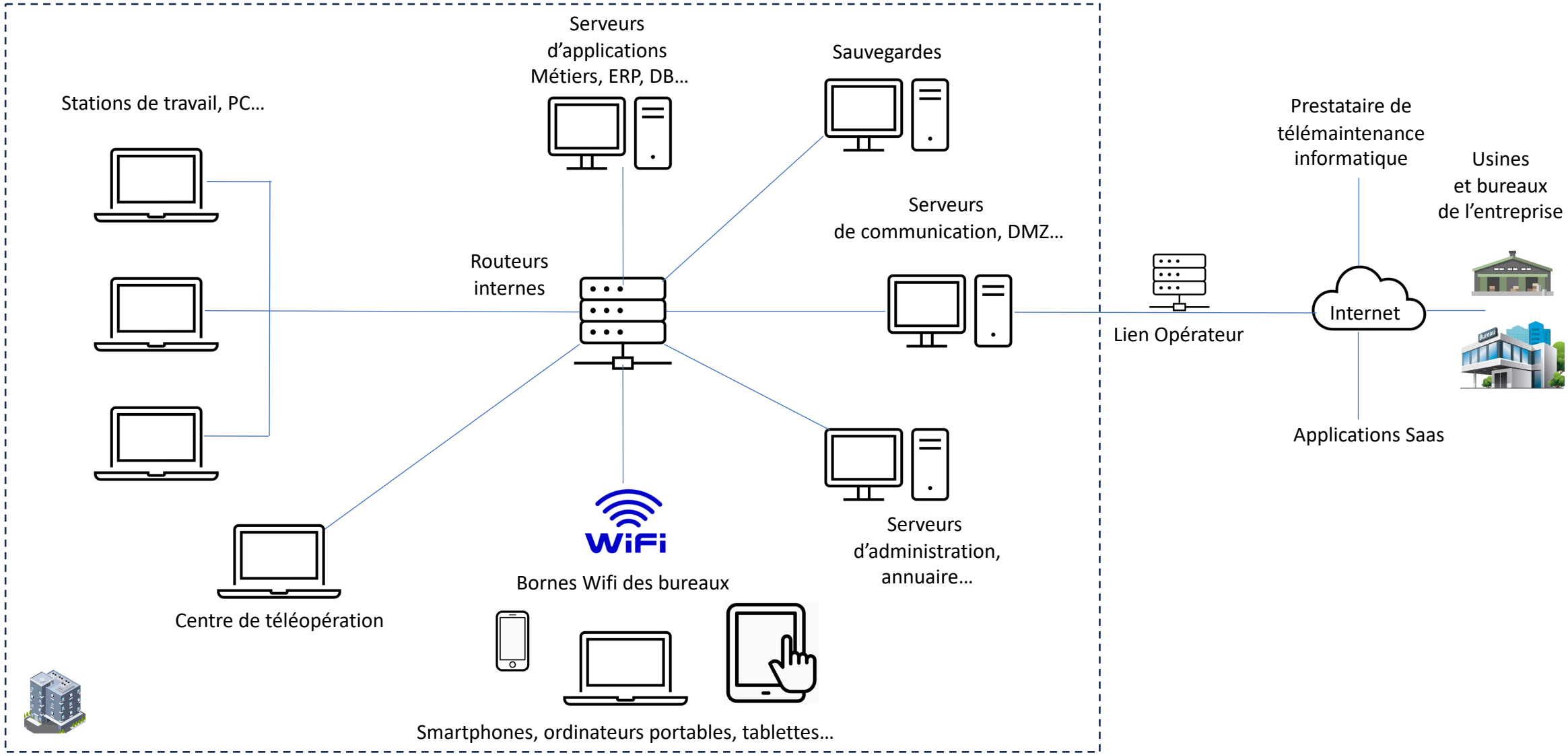
Implantations de l’entreprise

Siège

Usines

Bureaux

Schéma d’architecture réseau



Pour la Bleu Team: planification du SMSI *(Plan)*

- Appréciation et traitement des risques
- Objectifs de sécurité et plans pour les atteindre
  - Rappel:
    - Cohérents avec les résultats de l'appréciation et le traitement des risques
    - Mesurables avec des indicateurs KPI
- Ressources
- Compétences
- Sensibilisation
- Communication

Planification du SMSI: Appréciation des risques
Scénarios stratégiques de risques

SOURCES DE RISQUE	OBJECTIFS VISÉS	ÉVÉNEMENT REDOUTÉ	CHEMINS ATTAQUES STRATEGIQUES	GRAVITÉ
Concurrent	Vol de savoir faire	Intrusion dans les SI de SR	Intrusion dans les SI pour voler des information d'ingénierie robotique	
Etatique	Cheval de Troie dans les robots	Modification malveillante des codes des robots	Modification malveillante des codes des robots en ajoutant des chevaux de Troie	
Cyber criminels	Rançonnage	Injection de malware	Injection de malware pour rançonner la société SR	

Planification du SMSI: Appréciation des risques
Scénarios opérationnels de risques

CHEMINS ATTAQUES STRATEGIQUES	GRAVITE	CHEMINS ATTAQUES OPERATIONNELS	VRAISEMBLANCE
Intrusion dans les SI pour voler des information d'ingénierie robotique		R1: Intrusion pour voler des données en utilisant une vulnérabilité non corrigée sur un serveur frontal Internet	
		R2: Intrusion pour voler des données en utilisant un accès fournisseur externe vulnérable (mot de passe faible)	
		R3: Intrusion pour voler des données en utilisant une vulnérabilité 0 days sur un serveur frontal Internet	
Modification malveillante des codes des robots en ajoutant des chevaux de Troie		Modification des codes en ajoutant des chevaux de Troie par un développeur malveillant	
		Modification des codes en ajoutant des chevaux de Troie par corruption d'un logiciel de développement acheté	
Injection de malware pour rançonner la société SR		Injection de malware pour rançonner la société SR par phishing et chiffrement des postes de travail	

Planification du SMSI: Appréciation des risques
Echelle de gravité

ÉCHELLE	DÉFINITION
G4 – CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)
G3 – GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
G2 – SIGNIFICATIVE	Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
G1 – MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges)

Planification du SMSI: Appréciation des risques
Echelle de vraisemblance

ÉCHELLE	DESCRIPTION
V4 – CERTAIN OU DÉJÀ PRODUIT	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisation (historique d'incidents)
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 – PEU VRAISEMBLABLE	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

ENISA report (EU CERT), Top Cyber Threats

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Planification du SMSI: Traitement des risques

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Cout / Complexité	Echéance	Statut
Mesures organisationnelles						
Processus de gestion des vulnérabilités	R1	DSI	Rapidité d'application des correctifs	+	CT	
Surveillance des serveurs Internet, SOC	R3	RSSI	Cout Compétences	+++	MT	
PlanAssuSécu	R2	R.Juridique		+	CT	
Mesures techniques						
SIEM	R2	RSSI	Cout	++	MT	
Bastion accès fournisseur	R2	DSI		+	CT	

Planification du SMSI: Objectifs de sécurité

- Proposer des objectifs de sécurité pour votre SMSI
  - Appliquer les correctifs de sécurité, par ordre de priorité 1-frontaux Internet/ 2-serveurs internes/ 3-postes de travail
    - 80% du parc à S+1, 90 du parc à M+1, 100% du parc à M+3
  - Mettre en œuvre un SOC sur les actifs par ordre de priorité 1-frontaux Internet + bases de données Ingénierie + télépilotage Robot/ 2-serveurs internes + serveurs d'application Ingénierie/ stations de travail design robotique
    - 100% des Priorité1 à 6 mois, 100% des Priorité2 à 9mois, 100% des Priorité3 à 1an
  - Contractualiser avec tous les prestataires un Plan d'Assurance Sécurité (maintenance PC, DB brevet…) aligné sur les objectifs de sécurité e la PSSI
    - % de prestataires avec PAS vs sans PAS

Planification du SMSI: Ressources

- Décrire les ressources nécessaires:
  - Budget SMSI: licence d'un logiciel GRC pour gérer le SMSI, préparation du budget des licences des logiciels Cyber suite à l'évaluation des risques (anti-malware, SIEM., etc.), budget de l'équipe SSI, des prestataires externes si nécessaire
  - Délais: planification 2mois, documentation 6 mois, audit test 1 mois, audit de certification, plan de mise à jour
  - Qualité: tableau de bord de suivi de la mise en œuvre du SMSI, analyse des écarts, plan de correction, suivi en comité Cyber
  - Humain- Equipe projet SMSI: 1 responsable (RSSI), 1 chef de projet, équipe Cyber pour l'analyse des risques, la documentation et le suivi des projets Cyber

Planification du SMSI: Compétences

- Décrire les compétences nécessaires
  - 1 responsable SMSI (RSSI): formation ISO 27001 lead Implementer
  - 1 chef de projet: formation gestion de projet et sécurité,
  - Equipe SSI pour l'analyse des risques, la documentation et le suivi des projets SSI:
    - Administrateur Applicatif pour les tests fonctionnels sur les correctifs
    - Administrateurs système pour les tests techniques sur les correctifs
    - Responsable SOC
    - Analyste SOC niveau 1 & 2
    - Analyse CSIRT (forensics)
    - Analyste des menaces CTI
    - Auditeur organisation & sécurité physique pour la formalisation des PAS
    - …
  - 1 auditeur test SMSI : formation ISO 27001 lead Auditor

Planification du SMSI: Sensibilisation

- Décrire les actions de sensibilisation que vous prévoyez
  - Cours Cyber annuel certifiant pour tous les collaborateurs
  - Séance de sensibilisation pour les dirigeants sur les enjeux cyber financier, juridique, de réputation
  - Séance de sensibilisation pour les dirigeants sur les enjeux cyber opérationnel, avec préparation du processus « GPC »
  - Séance de sensibilisation à la PSSI pour les développeurs et la DSI
  - Campagne de faux phishing
  - Campagne d'affichage, de présentation d'évènement d'actualité, de jeux sérieux, d'objets promotionnels, etc.

Planification du SMSI: Communication

- Décrire les actions de communication que vous prévoyez:
  - Communiquer sur les menaces et les évolutions, le suivi des vulnérabilités, le niveau de sécurité et sa tendance, les incidents de sécurité et les enseignements, les projets en cours et à venir
  - Communiquer: lors des comités stratégiques, opérationnels, suivi des projets cyber suivant le cycle du SMSI (PDCA)
  - Communiquer avec la Direction, les directions métiers, l'IT, l'équipe cyber, les filiales, les partenaires en particulier en vue d'une crise cyber possible
  - Communiquer: par le responsable du SMSI, par le chef de projet, par les responsable d'activités cyber (SOC, CTi…)
  - Organiser le processus de communication cyber internet et externe, en temps normal et en temps de crise: identifier les acteurs et les responsables

Incident de sécurité à la SR

- H0= Appel téléphonique d'une filiale étrangère pour des difficultés de connexion à l'intranet de la SR
- H0+10mn: Appel téléphonique d'une autre filiale étrangère pour un écran vide avec un seul fichier *ReadMe*
- H0+15mn: Appel téléphonique d'un service interne pour l'écran ci-contre avec un compteur qui décrémente
- H0+18mn: La personne en charge de la communication à la SR vous informe qu'un mail a été reçu sur la boite aux lettres de contact externe s'intitulant *Payment for private key*
- H0+19mn: … vous prenez votre plan de gestion d'incident et des crise cyber: que contient-il ?

➢ Proposer les actions immédiates de votre plan incident cyber

Actions immédiates de votre plan Incident Cyber

- Liste des actions immédiates de réponse à l'incident et à l'organisation de la cellule de crise
  - Alerter la direction de l'entreprise – Mobiliser la cellule de crise et les cellules adhoc (communication, juridique…) - Prévenir les managers et donner les consignes des premières actions et de communication interne/externe
  - Mobiliser la cellule IT pour la gestion de l'incident (DSI, SSI, correspondants SSI en usine et dans les bureaux internationaux) - Prendre contact avec vos prestataires pour solliciter de l'aide suivant leurs compétences
  - Ouvrir une main courante des évènements dans chaque cellule pour le RetEx
  - Endiguer l'incident: isoler les réseaux pour éviter la propagation interne et externe, et rassembler les experts pour comprendre l'attaque en investiguant l'incident
  - Passer les consignes par SMS / GSM / téléphone aux employés dont la machine est infectée de ne pas éteindre les machines, de les isoler du réseau (retirer les câbles et/ou couper le Wifi, de les laisser alimentée en électricité
  - Préparer les communications internes et externes de crise – Messages clés, cibles, moyens de les envoyer
  - Préparer les modes de travail dégradé avec outils et procédures adaptés, éventuellement manuel, pour les directions de l'entreprise
  - Préparer la remédiation, le durcissement et la surveillance de l'IT à partir d'un cœur de confiance sain et son extension progressive