

<p>W</p>  <p>UIMM PROMEO LA FABRIQUE DE L'AVENIR</p>	<p>BTS Services Informatiques aux Organisations Opt SISR</p>	<p>Gabriel Pilarski</p> <p>SIO 26</p>
---	---	--

Projet Personnel Encadré

Numéro 2

Présentation du projet

1. Contexte de l'entreprise

L'entreprise fictive **TechSolutions** est une PME spécialisée dans le développement d'applications web. Elle compte une vingtaine d'employés et manipule des données sensibles liées à ses clients (identifiants, projets, documents internes).

Jusqu'à présent, l'infrastructure informatique de l'entreprise était fonctionnelle mais peu sécurisée. Aucune solution de supervision ni de centralisation des journaux n'était en place, et les politiques de sécurité étaient limitées.

2. Incident de sécurité

L'entreprise a récemment été victime d'une cyberattaque ayant entraîné une compromission partielle de son système d'information.

2.1 Origine de l'attaque

Un employé a reçu un email de phishing imitant un service interne. En cliquant sur un lien frauduleux, il a saisi ses identifiants professionnels, qui ont été récupérés par un attaquant.

2.2 Déroulement de l'attaque

Grâce aux identifiants compromis, l'attaquant a pu :

- Accéder au réseau interne de l'entreprise
- Effectuer une reconnaissance du réseau (scan des machines et des services)
- Identifier les serveurs critiques, notamment :
 - le contrôleur de domaine (Active Directory)
 - le serveur de fichiers
 - le serveur web

L'attaquant a ensuite tenté plusieurs actions malveillantes :

- Accès à des partages de fichiers contenant des documents sensibles
- Tentatives d'élévation de privilèges
- Multiples connexions suspectes sur le domaine

L'absence de supervision n'a pas permis de détecter rapidement ces activités. Suite à cet incident, la direction a décidé de renforcer la sécurité de son infrastructure.

L'entreprise TechSolutions a fait appel à une société spécialisée en cybersécurité nommée **Securos**. Cette entreprise externe a pour mission d'accompagner TechSolutions dans la sécurisation de son système d'information.

Dans ce cadre, Securos réalise un audit de l'infrastructure existante afin d'identifier les vulnérabilités exploitées lors de l'attaque. À la suite de cette analyse, elle met en place des solutions adaptées, notamment l'implémentation d'outils de supervision et de centralisation des logs tels que Zabbix et Graylog, ainsi que l'application de bonnes pratiques de sécurité.

Securos assure également un suivi continu de l'infrastructure, permettant de détecter rapidement toute activité suspecte et de garantir une meilleure protection contre de futures attaques.

3. Objectifs du projet

L'objectif de ce projet est de :

- Reconcevoir une infrastructure sécurisée
- Mettre en place des outils de supervision et de journalisation
- Détecter les comportements anormaux
- Réagir efficacement en cas d'incident
- Prévenir de futures attaques

4. Infrastructure de l'entreprise

4.1 Équipements réseau

- Un switch
- Un poste client

4.2 Serveurs

Contrôleur de domaine

Un serveur Windows Server avec les rôles suivants :

- Active Directory : gestion centralisée des utilisateurs et des droits
- DNS : résolution de noms interne

Serveur Web + zabbix

Un serveur Linux (Ubuntu) héberge le site web de l'entreprise et sert également de poste Zabbix.

Serveur Graylog

Un serveur Linux (Ubuntu) héberge le logiciel Graylog de l'entreprise.

5. Mise en place de la supervision

Afin de détecter rapidement toute activité suspecte, des outils de supervision ont été déployés.

5.1 Supervision des équipements

L'outil Zabbix a été mis en place pour surveiller :

- L'utilisation CPU et mémoire des serveurs
- L'état des services
- La disponibilité des machines

Des alertes sont générées en cas de comportement anormal.

5.2 Centralisation des logs

L'outil Graylog a été installé pour :

- Collecter les journaux des serveurs.
- Analyser les connexions
- Détecter des tentatives d'intrusion

Grâce à cet outil, il est possible d'identifier :

- Des connexions échouées répétées
 - Des accès inhabituels
 - Des comportements suspects
-

8. Conclusion

Ce projet a permis de mettre en évidence l'importance de la cybersécurité au sein d'une entreprise.

La mise en place d'une infrastructure sécurisée, associée à des outils de supervision comme Zabbix et Graylog, permet :

- Une meilleure visibilité sur le système d'information
- Une détection rapide des incidents
- Une réaction efficace face aux menaces

Ce PPE illustre les bonnes pratiques en matière de sécurisation des systèmes et des réseaux dans un contexte professionnel réel.

ANNEXE :

Zabbix :

The screenshot displays the Zabbix web interface for configuring hosts. The left sidebar contains navigation menus for Dashboards, Monitoring (Problems, Hosts, Latest data, Maps, Discovery), Services, Inventory, Reports, Data collection, Alerts, Users, Administration, Support, and Integrations. The main content area is titled 'Hosts' and includes a 'Create host' button. Below the title is a form for adding a new host with the following fields and options:

- Name:
- Host groups: type here to search
- IP:
- DNS:
- Port:
- Status: Any Enabled Disabled
- Tags: tag value
- Show hosts in maintenance:
- Show suppressed problems:
- Severity: Not classified Warning High Information Average Disaster
- Buttons:

Below the form is a table listing existing hosts:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
linux-client	192.168.50.111:10050	ZBX	class: os target: linux	Enabled	Latest data 68	2	Graphs 14	Dashboards 3	Web
WIN-LSMBU737308	192.168.50.110:10050	ZBX	class: os target: windows	Enabled	Latest data 113	2	Graphs 12	Dashboards 3	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software subclass: logging	Enabled	Latest data 167	1	Graphs 20	Dashboards 4	Web

Displaying 3 of 3 found