zenika

Votre entreprise est-elle vulnérable aux attaques physiques ?

Retour d'expérience
d'une mission Red Team
chez Great Place To Work® France

Sommaire

Avant-propos

Ce cas d'usage est le retour d'expérience d'une mission effectuée par l'équipe ZenSec de Zenika, nos spécialistes en cybersécurité, et du Directeur des Systèmes d'Information chez Great Place To Work® France.

Pour des raisons évidentes, nous ne rentrerons pas dans les détails des failles exploitées pour ne pas divulguer d'informations sensibles notamment sur l'infrastructure informatique de Great Place To Work® France.

Qu’est-ce qu’une Red Team ?

Une Red Team est une équipe de hackers autorisée qui a pour but de récupérer des données de l’entreprise ou d'atteindre des cibles définies en amont par le client et la Red Team pour simuler une attaque réelle.

Ces objectifs peuvent être variés et diffèrent selon les failles identifiées et considérées comme potentiellement critiques : entrer dans des locaux, récupérer un disque dur, voler un ordinateur, déposer une boîte de chocolats sur le bureau de la Direction...

“Au quotidien, les principales lacunes de sécurité constatées par le Centre de cyberdéfense sont :

- des systèmes et des applications, dont les sites Web, qui ne sont pas à jour de leurs correctifs de sécurité
- une politique de gestion des mots de passe insuffisante (mots de passe par défaut ou trop simples et non renouvelés régulièrement…)
- une absence de séparation des usages entre utilisateur et administrateur des réseaux
- un laxisme manifeste dans la gestion des droits d’accès
- une absence de surveillance des systèmes d’information (analyse des journaux réseaux et de sécurité)
- un cloisonnement insuffisant des systèmes qui permet à une attaque de se propager au sein des réseaux
- une absence de restrictions d’accès aux périphériques (supports USB…)
- une ouverture excessive d’accès externes incontrôlés au système d’information (nomadisme, télétravail ou télé administration des systèmes)
- une sensibilisation et une maturité insuffisantes des utilisateurs et des dirigeants face à la menace dont ils ne perçoivent pas les risques.”

Source : ANSSI

Enjeux et objectifs de la mission

Mettre en place cette mission Red Team a découlé de plusieurs pentests* effectués en amont par l'équipe ZenSec sur les applications de Great Place To Work® France disponibles sur le Web. Ces pentests ont permis d'identifier certaines failles et de renforcer la sécurité du point de vue des attaques distantes.

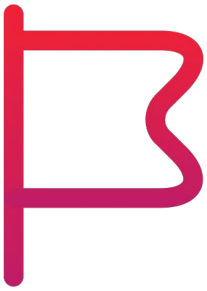
Un point d'interrogation restait cependant en suspens : **les attaques physiques. L'entreprise était-elle capable de les contrer ?**

Un peu d'historique
Avant même la mission, une tentative d'intrusion dans les locaux avait été tentée par une personne se faisant passer pour quelqu'un qu'elle n'était pas. Cette intrusion a été évitée un peu par manque de préparation de l'intrus et un peu par chance, selon la DSI de Great Place To Work France ©.

*voir page 17

Cette tentative d'intrusion et les différents pentests effectués ont conforté la DSI dans la mise en place du Red Teaming pour **tester la sécurité des locaux avec une intrusion physique plus travaillée et plus ciblée** afin de :

- tester des failles déjà identifiées,
- déterminer à quel point elles étaient exploitables
- déterminer les actions prioritaires à mettre en place
- déterminer les moyens nécessaires



Mais aussi :

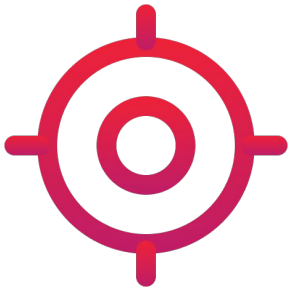
- **sensibiliser les collaborateurs**

Cette sensibilisation est primordiale, car la plupart des attaques (distantes ou physiques) sont possibles suite à des erreurs et comportements humains.

Cibles de la Red Team et préparation

Quelles étaient les cibles de l'équipe ZenSec ?

Avant de démarrer la mission, il était nécessaire de déterminer les cibles de l' équipe ZenSec :



- 🎯 Entrer dans les locaux
- 🎯 Entrer dans la salle serveur et récupérer des ordinateurs laissés spécifiquement pour la mission
- 🎯 Déposer des backdoors physiques dans l'entreprise
- 🎯 Déposer des clés USB et analyser le comportement des employé·es face à une clé inconnue

Ces cibles peuvent sembler anodines mais permettent de mettre en lumière les différentes failles qui permettent d'atteindre ces cibles.

*voir page 17

Comment l'équipe s'est-elle préparée à la mission ?

Une fois les cibles définies, la phase de préparation peut commencer.

Il s'agit surtout d'obtenir le plus d'informations possibles sur la cible. Cela passe donc par beaucoup d'observation :

- **Observation à distance :** recherche d'informations disponibles sur le web photos des locaux...
- **Observation sur site :** analyse des entrées/sorties, identification de potentiels partenaires de l'entreprise...

L'objectif est d'avoir une bonne compréhension des locaux et de l'écosystème de l'entreprise.

Cette étape permet également à l'équipe de définir le matériel dont elle aura besoin pour s'introduire dans le bâtiment et atteindre ses cibles.

La RedTeam a-t-elle atteint ses cibles ?

Oui.

✅ Entrer dans les locaux

> **La première des failles exploitée**, et peut-être celle à laquelle on pense le moins, a été **la confiance** des employé·es de l'entreprise : l' équipe d'intrus a pu entrer dans les locaux sans que personne ne vérifie vraiment leur identité.

Une fois entrée, l'équipe a plutôt facilement pu accéder au reste des cibles.

✅ Entrer dans la salle serveur et récupérer des ordinateurs laissés spécifiquement pour la mission

> Cette cible a été atteinte grâce à une autre faille humaine, **la recherche de la facilité.**
> À l'époque des faits, les clés de la salle serveur étaient accessibles à toute personne qui se trouvait dans le bâtiment pour 2 raisons très simples :
>
> - Selon les employé·es, il était plus simple de laisser les clés à disposition plutôt que de demander à quelqu'un d'ouvrir la salle.
> - Les employé·es avaient **confiance** en la sécurité du bâtiment. Or la première cible a été atteinte car ces mêmes employé·es n'ont pas été assez méfiants.

✅ Déposer des backdoors physiques

Laisser les back doors a été plutôt simple une fois dans le bâtiment et dans la salle serveur. Ces back doors ont pu être utilisées pour entrer dans le réseau à distance.

✅ Déposer des clés USB et analyser le comportement des gens face à une clé inconnue

L'atteinte de cette cible est sans doute due à plusieurs failles humaines : **la confiance dans les outils et objets** présents dans l'entreprise**, la facilité d'usage** (j'ai besoin d'une clé USB maintenant), **et la curiosité** :

- Les clés USB contenaient un fichier nommé "Paie" qui a été ouvert plusieurs fois.

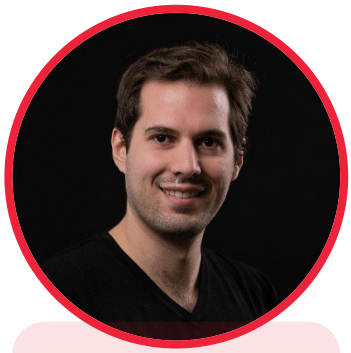
Failles supplémentaires identifiées

🔑 **Accès à la badgeuse** : la Red Team aurait pu se créer des badges tout à fait valides.

🔑 **Vol de quelques mots de passe** qui auraient pu servir à une attaque.

Résultats de la mission

Avant de parler des résultats



Xavier Detant, DSI

GPTW France ©

Bonne pratique

“Je n'avais pas prévu de faire ça, mais après l’attaque et avant la restitution, une personne convaincue du bien-fondé de la présence de la Red Team dans les locaux est venue me parler de ce qu’a fait ladite équipe. Je lui ai alors dévoilé qu’elle avait été piégée et qu’il s’agissait d’une attaque organisée en secret.

Cette personne pouvait faire ce qu’elle voulait de cette information : la garder pour elle ou en parler.

Au moment de la restitution, la plupart des gens étaient au courant de l’attaque et savaient qu’ils s’ étaient fait piéger.
L’information venant d’une personne non-tech, les autres personnes ont pris conscience qu’elles auraient pu être piégées elles aussi.

Cela a permis à chacun d’être plus ouvert et de ne pas vivre la restitution comme un échec mais plutôt comme un apprentissage.”

Revenons aux résultats.

✅ Un changement de culture et de mentalité

Le Red Teaming a permis **un changement dans la culture de la sécurité et une prise de conscience du risque :** les collaborateurs·i-rices ont naturellement abordé le sujet pendant les pauses-café, les déjeuners...

Cette mission a permis à la DSI d'être écoutée et entendue. En effet, les employé·es de l'entreprise ayant été confronté·es à la pratique et pas simplement à la théorie, on met fin aux réactions du type : "Oh ça va ! Ils exagèrent."

✅ Un renforcement des outils et des process

Peu de temps après la mission, et avant la réunion de restitution, l'équipe n'a pas pu entrer aussi facilement dans les locaux de l'entreprise : ils ont été confinés à un endroit en attendant que leur contact vienne à leur rencontre.
Les équipes se sont responsabilisées d'elles-mêmes suite à la mission (voir encart : "Bonne Pratique" à la page précédente)

D'autre part, l'accès aux points critiques a été sécurisé (salle serveur, badgeuse)

Points inattendus à prendre en compte quand on commandite une Red Team

Gestion du secret

La mise en place de ce genre de mission montre quelques difficultés à prendre en compte.
Il est bien évidemment difficile de garder le secret avant la mission, surtout dans une entreprise très transparente. Cependant, **il est important de ne rien divulguer avant le début de celle-ci sous peine de fausser les résultats.**

Dans le cas de cette mission, le DSI a choisi de révéler la mission à une seule personne qui était venue lui en parler (cf. page 12), ce qui a été bénéfique dans le cadre de Great Place to Work® France, mais c'est à vous de juger si oui ou non cela est pertinent dans votre situation, si le cas venait à se présenter.

Après la mission, il peut être utile d'en discuter avec les collaborateurs·rices pour lever les inquiétudes.

Gestion du temps et organisation

Le plus difficile reste l'organisation, car la préparation de **ce type de mission prend du temps, mais du temps caché !**

En gros, sur le papier et en termes de communication interne avec vos équipes, vous avez du temps, mais en réalité non, puisque vous préparez l'attaque secrète de votre entreprise. C'est un aspect à prendre en compte pour vous organiser au mieux.

zenika

Zenika est un cabinet de conseil IT qui accompagne les entreprises dans leur transformation numérique, implanté en France, au Canada, à Singapour et au Maroc.

Lien entre le monde organique et le monde numérique, notre expertise commence par une interface et s'achève au stockage de la donnée et son exploitation, en mode agile, devops, et sécurisé.

Partage, transparence et convivialité sont des valeurs qui portent Zenika, c'est donc naturellement, que notre communauté s'engage fortement dans l'open source et le numérique responsable.

Découvrir Zenika

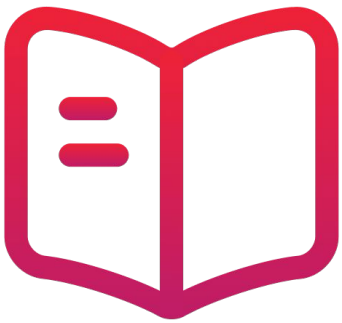
Great Place To Work® est la référence mondiale en matière d'expérience collaborateur.

Depuis 1992 dans le monde et 2002 en France, nous avons interrogé plus de 100M de salariés à travers 60 pays. Leurs réponses nous ont permis de déterminer ce qui définit une expérience collaborateur de qualité. Au cœur de cette réussite, on retrouve une notion clé : la confiance. C'est sur la confiance que nous avons fondé une méthodologie unique, qui nous permet d'aider les organisations à créer un environnement de travail inclusif, à piloter leur stratégie RH et à améliorer leur performance.

Great Place To Work®

Nous distinguons les organisations où il fait bon travailler grâce à notre Certification et à la publication annuelle de notre Palmarès Best Workplaces™.

Glossaire



Pentest :

Penetration Test ou Test d'intrusion. Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs.

Remarques : Il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information).

Backdoor :

Porte dérobée. Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive.

Remarques : Une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole.

(Source : ANSSI)

Merci à

Xavier Detant, DSI @ Great Place to Work® France
et **Jean-Baptiste Caron**, Pentesteur @ Zenika,
pour le temps accordé dans la rédaction de ce cas d'usage