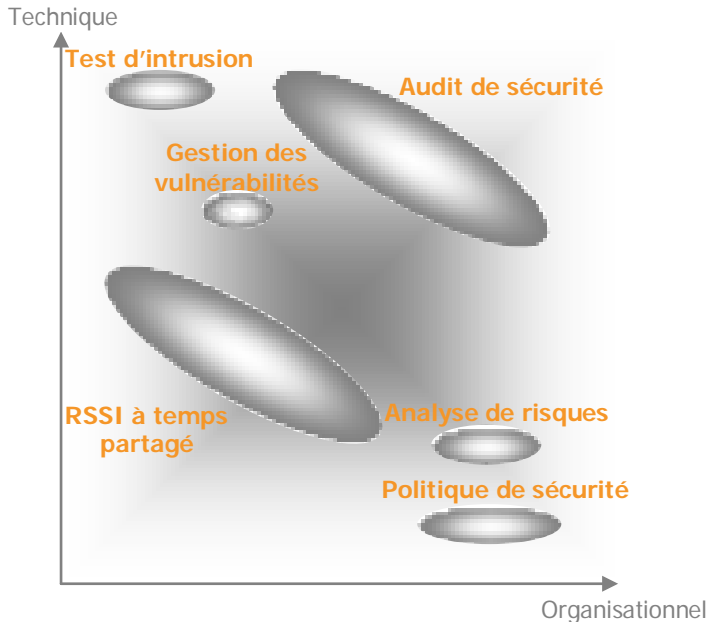


## AUDIT TECHNIQUE DE SECURITE, CAMPAGNE DE TEST D'INTRUSION ET GESTION DES VULNERABILITES :

« MESURER ET SE MESURER A SON SI POUR SE PREMUNIR »



Les différents volets abordés dans cette communication : **audits de sécurité, test d'intrusion et gestion des vulnérabilités techniques**, sont des prestations de sécurité à caractère très technique.

Intrinsec réalise d'autre part des prestations de sécurité à caractère plus organisationnel telles que des **analyses de risque**, ou des productions de **politiques de sécurité**.

Pour ce qui est de la prestation '**RSSI à temps partagé**', elle englobe elle les 2 aspects, technique et organisationnel d'une manière globale.

L'équipe d'ingénieurs en sécurité informatique d'Intrinsec est un pôle très spécialisé au sein de notre société. Composée d'une dizaine de collaborateurs à fort potentiel, ils sont garants de nos propres infrastructures, pour la sécurité informatique des clients hébergés auxquels nous offrons un service haut de gamme. Ces ingénieurs en sécurité informatique réalisent aussi des prestations de sécurité pure auprès de sociétés qui nous témoignent leur confiance.

À cette fin, nous nous dotons des meilleurs profils en la matière sur le marché. Lors de leur recrutement, un véritable état d'esprit est exigé par les plus anciens qui ont fait la notoriété d'Intrinsec à ses débuts. Une vraie capacité à se mettre dans la peau d'un pirate informatique nourrissant une volonté forte de détourner des systèmes quels qu'ils soient, une grande pro activité dans l'identification d'idées malveillantes, une capacité à se mettre dans la peau d'un mercenaire tout esprit mal tourné et tortueux qu'il ait, à envisager n'importe quelle fraude, escroquerie, falsification, tricherie, voilà les pré-requis pour faire partie de l'équipe des ingénieurs en sécurité informatique à Intrinsec.

### REACTION SUR INCIDENT

Il peut arriver que l'un de nos ingénieurs en sécurité informatique soit appelé en urgence

parce qu'une intrusion a été détectée sur un système, c'est en général l'état d'urgence, il faut réagir immédiatement, le week-end, la nuit, n'importe quand, pour collecter des preuves, diagnostiquer l'événement et sa cause, et mettre le client en relation avec les autorités compétentes pour l'aider à faire ses démarches, porter plainte par exemple.

Pour une attaque virale, l'ingénieur en sécurité informatique fait un état des lieux, cantonne la diffusion, nettoie le système et essaie de remettre globalement les systèmes en route. Il recherche ensuite de quelle manière le virus a réussi à pénétrer. Cette dernière action est primordiale puisqu'elle permet parfois de mettre en lumière un problème organisationnel interne.

Si réagir s'avère parfois nécessaire, prévenir ce type d'incidents, et aider un client à se prémunir contre toute malveillance potentielle visant son SI reste la mission principale d'un ingénieur en sécurité informatique de notre équipe.

### AUDIT DE SECURITE

Un audit de sécurité est une démarche collaborative entre notre ingénieur en sécurité informatique et les différents acteurs de la société audité, un partage des connaissances : lui, apporte son expertise en matière de sécurisation du SI et de processus de gestion de la sécurité informatique, eux, le

contexte métier spécifique et la stratégie en matière de sécurité informatique de la société. La démarche s'adapte à la taille, à la complexité, au métier de l'entreprise tout en s'appuyant sur les normes ISO 27001 et 27002. Au regard de tous ces éléments, l'ingénieur en sécurité informatique construit un référentiel de bonnes pratiques couvrant les aspects : gestion du contrôle d'accès, des incidents de sécurité informatique, du maintien en conditions opérationnelles, de la continuité de service, de l'exploitation courante, des télécommunications, de la gestion des biens, de la conformité légale (propriété intellectuelle, de la vie privée...) etc.

Suite aux entretiens et aux sessions de travail qu'il organise, l'ingénieur en sécurité informatique confronte les pratiques du client vis-à-vis du référentiel préalablement établi. En parallèle l'ingénieur réalise un audit de sécurité technique visant à :

- analyser toutes les strates du SI depuis l'architecture jusqu'aux éléments de configuration,
- mettre en avant les écarts entre d'une part : les informations collectées lors des entretiens et leur réalité sur le SI, d'autre part entre les pratiques de la société en matière de sécurité informatique et ce que l'on constate de l'état de l'art.

Un état des lieux (forces et faiblesses) de l'existant en termes de sécurité informatique est réalisé, ainsi qu'un ensemble de préconisations structurées dans un schéma directeur mettant en évidence des « Quick Wins » (chantier d'améliorations très court terme à forte valeur ajoutée), des travaux à court, moyen et long terme, et tenant compte des priorités, des budgets alloués. L'ingénieur en sécurité informatique analyse le contexte de son intervention et prend en compte les projets connexes et structurants dans sa démarche d'audit de sécurité (par exemple : une démarche ITIL, un plan de reprise d'activité, un projet d'externalisation...).

En back office nos ingénieurs en sécurité informatique maintiennent un niveau de compétence perpétuellement à jour sur l'ensemble des problématiques de sécurité informatique, une veille technologique dont nos clients sont les bénéficiaires directs.

En outre, le collaborateur Intrinsec s'efforce lors de sa mission à sensibiliser l'ensemble des acteurs rencontrés et à véhiculer les idées, les valeurs et la démarche de sécurité informatique qui est celle de l'entreprise, afin de créer l'adhésion et rendre son action bénéfique et efficace.

## TEST D'INTRUSION

Beaucoup plus démonstratif que l'audit de sécurité informatique, le test d'intrusion (TI) est un autre vecteur de sensibilisation. Lorsque notre ingénieur en sécurité informatique œuvre en interne chez un client sur de l'écoute téléphonique par exemple, et qu'il remet 3 fichiers mp3 d'une conversation entre la direction sur site, et un autre directeur informatique à l'étranger, bien sûr ça ne fait pas plaisir, mais le message est fort. Lorsqu'il accède aux emails d'un VIP ou d'un DSI en passant simplement par le web, c'est très démonstratif aussi.

Les campagnes de Test d'Intrusion constituent un autre volet du travail de l'équipe des ingénieurs en sécurité informatique d'Intrinsec. Le succès de ces campagnes réside dans la capacité des ingénieurs en sécurité informatique à se positionner dans la peau d'un attaquant. Ils utilisent exactement les mêmes méthodes et techniques qu'un pirate informatique, mais dans un cadre complètement légal puisqu'ils sont mandatés par les entreprises pour soumettre un système (ou un périmètre) à un certain niveau d'attaque durant un certain temps.

On parle d'un niveau d'attaque pour le test d'intrusion. Celui-ci fait référence en réalité à la dangerosité d'un attaquant qui peut être un informaticien lambda plus ou moins expert, comme un mercenaire qui a du temps et beaucoup d'argent à consacrer à l'opération. On parle aussi du temps consacré au test d'intrusion, c'est en effet un paramètre structurant en raison du fait qu'un bon nombre d'attaques soit limité par le temps qu'on y consacre.

4 types de test d'intrusion peuvent être réalisés :

**Test d'intrusion Internet :** L'ingénieur en sécurité informatique tente de pénétrer l'infrastructure depuis le réseau Internet, il peut être n'importe où et attaquer le système sur son périmètre exposé à l'extérieur : applications web, serveurs de mails, etc.

**Test d'intrusion interne :** Ce test d'intrusion couvre le potentiel de malveillance

d'un utilisateur en interne, un 'intruder'. L'ingénieur en sécurité informatique s'assimile à un pirate qui rentre dans les locaux ou un utilisateur malveillant et se connecte à l'infrastructure. L'ingénieur va référencer tout ce qu'il est capable de faire après s'être connecté. S'il arrive à rentrer en profondeur dans l'infrastructure, il évalue son potentiel de rayonnement dans l'infrastructure.

**Test d'intrusion sur les réseaux sans fil :** L'ingénieur en sécurité informatique cherche tous les réseaux visibles, évalue sa capacité à s'introduire sur le réseau, celle d'avancer plus avant dans l'infrastructure, et à dégrader son niveau de sécurité informatique. À l'insu des utilisateurs il tente de forcer leur connexion à un réseau sous son contrôle. Après avoir testé toutes ces intrusions, il dresse une liste des types/criticités des données qu'il est capable d'intercepter.

**Test d'intrusion sur les infrastructures télécom :** L'ingénieur passe par les réseaux téléphoniques ; modems de maintenance, serveurs téléphoniques pour s'assurer qu'ils ne représentent pas des points d'entrées directes contournant le périmètre de défense.

Il y a 3 approches correspondantes au niveau de connaissance du SI que l'on donne à l'ingénieur en sécurité informatique en charge de la campagne de test d'intrusion, selon qu'on veuille simuler le potentiel d'un attaquant : qui n'a aucune information concernant la société, qui a obtenu des informations de la part d'un 'insider' ou qui possède une bonne connaissance de la structure.

**Boîte noire :** L'ingénieur en sécurité informatique n'a que le nom de la société. Il consacre un certain temps à la collecte d'informations sur Internet afin trouver des équipements, des noms d'utilisateurs, etc. lui permettant de s'introduire sur l'infrastructure. Lorsqu'il est capable de définir un périmètre potentiel pour réaliser ses attaques, il le valide avec son client, car il a un cadre légal à respecter et ne peut pas prendre l'initiative d'attaquer sans l'accord de ce dernier.

**Boîte grise :** L'ingénieur en sécurité informatique possède quelques informations, l'adresse d'un site par exemple.

**Boîte blanche :** Le client fournit à l'ingénieur en sécurité informatique les schémas d'infrastructure afin qu'il détermine toutes les relations entre les équipements et qu'il comprenne rapidement quels scénarii de test d'intrusion sont intéressants.

Quand l'ingénieur en charge de la campagne de test d'intrusion sait s'introduire sur l'infrastructure, celui-ci ne se contente pas de dresser une liste des failles de sécurité informatique. Il émet des recommandations et préconise des actions concrètes de sécurisation.

Il n'est pas rare de trouver des vulnérabilités liées à la conception ou au développement des applications web : les sites de vente en ligne par exemple. Un individu malveillant peut réussir à accéder et exploiter des fichiers qui ne sont pas censés être visibles par l'utilisateur. Il peut aussi détecter des failles dans le workflow de l'application : se connecter au site, faire sa recherche, ajouter des produits à son panier, renseigner son identité, mais déclencher la livraison et se faire livrer, en contournant l'étape de paiement. Pour détecter ce type de failles l'ingénieur en sécurité informatique doit

posséder une bonne compréhension des processus métiers supportés par les applications, il doit déterminer les zones applicatives critiques, détecter les fonctionnalités qui présentent un intérêt en termes de malveillance financière par exemple, construire des scénarii de test d'intrusion combinant vulnérabilités techniques et contournement de workflow. L'exemple de la vente en ligne, est un exemple parmi d'autre, mais le problème se pose aussi pour les sites de vote en ligne, de gestion documentaire, des extranets, des sites institutionnels, etc.

## GESTION DES VULNERABILITES TECHNIQUES

Les vulnérabilités techniques sont des failles détectables de manière automatisée. Pour celles-ci, l'ingénieur en sécurité informatique utilise un outil qui scanne en masse tous les équipements d'un périmètre donné du SI et produit un rapport. Ce rapport, très dense en termes d'informations techniques, liste toutes les vulnérabilités potentielles par composant du périmètre scanné et par type de vulnérabilité. Leur est adjointe une criticité allant de 1 à 5 qui traduit l'impact de l'exploitation de la faille ainsi qu'un code couleur qui précise si ces vulnérabilités sont potentielles (et nécessitent une vérification manuelle afin d'être avérées) ou avérées de manière certaine.

L'ingénieur analyse et synthétise ce rapport afin de mettre en évidence les carences transverses en termes de gestion technique de la sécurité informatique du périmètre, qui débouchent généralement sur des préconisations de type gestion des correctifs ou patches. Il s'intéresse également de manière plus verticale à des composants du SI qui présentent beaucoup de vulnérabilités critiques avérées et qui donnent lieu cette fois à des préconisations de type reconfiguration de l'équipement.

Le scan et l'analyse du rapport de scan n'ont qu'une valeur d'état des lieux, il est ensuite nécessaire de mettre en place des actions de sécurisation du SI au niveau des composants du périmètre scanné. Si certaines vulnérabilités techniques peuvent être corrigées de manière ponctuelle et définitive, la plupart nécessitent la mise en place de processus à part entière afin de rendre systématiques certaines actions de sécurisation. Ces processus peuvent être plus ou moins lourds à mettre en place selon la complexité organisationnelle de la société et l'étendue du périmètre du SI considéré. Pour ce faire, les sociétés peuvent être accompagnées par nos ingénieurs en sécurité informatique.

La gestion des vulnérabilités techniques englobe la mise en place d'un plan d'amélioration continue nécessitant la pose d'indicateurs afin de suivre l'évolution du niveau de sécurité du périmètre du SI. Si les processus de sécurité informatique et les actions de sécurisation sont mis en œuvre, on constate au fil des scans (réalisés de manière régulière) l'évolution du niveau de sécurité informatique du périmètre au niveau de ses vulnérabilités techniques.