

a ■ LE REPÉRAGE

Il s'effectue très communément en plusieurs étapes d'approches successives.

Il faut tout d'abord que l'attaquant analyse le périmètre de l'entreprise, de même que son environnement direct, afin de savoir comment les locaux sont protégés et entretenus.

L'objectif immédiat étant de déceler des failles éventuelles à exploiter dans le dispositif de sécurité :

- Y a-t-il une clôture de sécurité électrifiée ?
- Si oui, peut-on la franchir sans risque, l'escalader ou la contourner ?
- Existe-t-il des brèches dans les clôtures ?
- Existe-t-il un dispositif de vidéosurveillance relié à une équipe de gardiennage ?
- L'équipe de gardiennage a-t-elle des postes fixes ou exécute-t-elle des rondes de surveillance ?
- Quels sont ses moyens de communication ?
- Quelles sont les heures de passage, le nombre de rondes, quand ont lieu les relèves ?
- Existe-t-il un accès visiteurs ou employés, dérobé ou moins surveillé ?
- Peut-on y accéder par un parking de stationnement ?
- Existe-t-il des horaires et des procédures de livraison de matériels divers ?
- Qui enlève les ordures et de quelle façon ?
- Celles-ci sont-elles enlevées à l'intérieur de l'enceinte des locaux ou sur une plate-forme extérieure de chargement ?
- Des poids lourds réalisent-ils des chargements ou des déchargements réguliers ?
- Etc.

Autant de questions essentielles qui permettront au professionnel de la pénétration sur site d'orienter sa stratégie d'approche et de planifier scrupuleusement son intrusion dans les lieux.

Une fois rendu dans l'enceinte de l'entreprise, il doit trouver un point d'accès pour pénétrer dans les locaux proprement dits.

Pour cela, il :

- analysera toutes les entrées possibles (entrées de service, entrées principales, entrées annexes, entrées dérobées, sas de déchargement, débarcadères de poids lourds, plate-forme d'accès, etc.) ;

- se demandera s'il y a des fenêtres au rez-de-chaussée (si oui, sont-elles protégées par des grilles ou des montants solides ?) ;
- vérifiera si l'entreprise utilise des vitres sécurisées et renforcées ;
- vérifiera si ces entrées et ces fenêtres sont toutes couvertes par de la vidéosurveillance ;
- se demandera si l'on peut désactiver la vidéosurveillance en coupant les câbles ou l'alimentation EDF du secteur ;
- se demandera s'il est possible d'escalader la façade jusqu'à un accès dérobé ;
- se demandera si une brèche évidente et opportune peut être décelée (une fenêtre laissée ouverte est l'exemple le plus fréquent, battant non verrouillé, etc.) ;
- observera s'il existe un moyen d'accéder et de pénétrer par une persienne sur le toit ;
- observera à nouveau les allées et venues du personnel de gardiennage, à l'intérieur de l'enceinte du site et des locaux de l'entreprise.

b ■ LE CROCHETAGE DE SERRURES

Cette opération bien connue désigne une manière technique d'ouvrir les serrures d'une porte close et sécurisée moyennant l'emploi d'appareils mécaniques de haute précision. Le point essentiel qu'il convient de toujours garder à l'esprit est que chaque type de serrure contient en lui-même le moyen d'être défait ou fracturé.

Selon la nature et le type de serrure utilisée, le crochetage sera plus ou moins complexe à exécuter. Il existe, sur Internet, de nombreux manuels pratiques formant à la mise en œuvre de ces techniques intrusives. Elles sont donc simples d'accès. Il est pourtant nécessaire, pour l'attaquant, de s'entraîner préalablement, car la prise en main n'est pas toujours aisée. Ces opérations très techniques demandent une très grande qualification pour être efficaces en un tour de main. Voilà pourquoi elles sont le fait de professionnels très spécialisés et dûment commandités, qui interviennent à la demande.

Enfin, il existe des « pistolets crocheteurs » qui facilitent la maîtrise rapide des procédés d'ouverture intrusive. Les agents du FBI américains en sont équipés en cas d'opérations spéciales nécessitant une pénétration immédiate dans les lieux. On peut très facilement s'en procurer sur Internet. Notamment sur le site www.southord.com.