Cyberattaques, ce risque réel loin d'être virtuel

A l'heure du BIM, des logiciels de calculs, simulation et visualisation, et des échanges par mail indispensables à l'exercice de la profession d'architecte, la menace digitale n'a jamais paru aussi importante. Les agences d'architecture sont-elles menacées ? Comment ouvrez-vous la fenêtre au virus sans le savoir ? Quelles solutions pour vous protéger ? Eléments de réponse.
Hollywood a inculqué dans l'imaginaire collectif la vision d'une tête de mort affichée à l'écran de l'ordinateur comme traduction d'une cyberattaque. La réalité est moins manichéenne, et au quotidien, de nombreux signes doivent vous mettre sur la piste de la méfiance et des bonnes pratiques à adopter :

- Votre ordinateur affiche un message indiquant que votre ordinateur est bloqué, planté ou qu'il est infecté par un virus et qu'il faut appeler un numéro de téléphone ?
- Google interdit l'accès à votre site web pour cause de contenu dangereux ?
- Vos recevez trop de mails de spams, de chantages à la webcam, ou de demandes de connexion à votre compte en banque ?
- Vos correspondants ne reçoivent plus vos emails car votre serveur de mail est blacklisté dans plusieurs blacklists ?
- La page de démarrage de votre navigateur a été changée ?
- Votre antivirus s'emballe et vous signale un grand nombre d'alertes ?
- Vous retrouvez des informations confidentielles en accès libre sur Internet ?
- Vous avez reçu un mail d'Hadopi alors que vous n'avez pas effectué de téléchargement illégal ?

Vous vous reconnaissez dans une de ces situations ? Alors vous êtes sûrement l'objet d'une attaque. Si l'expérience est désagréable, vous êtes (très) loin d'être un cas isolé. Ce serait même plutôt l'inverse avec une généralisation des cyberattaques au sein d'entreprises toujours plus nombreuses à détecter une tentative d'intrusion. Plus nombreuses mais de combien ? 20 % ? 40 % ?
Bien plus … Selon Opinion Way*, 70% des entreprises ont été victime au moins une fois d'une tentative d'intrusion, conduisant dans 30% des cas à une fraude avérée. Au total, dans 1 cas sur 4, la cyberattaque conduit à un arrêt partiel de l'activité.
Des conséquences lourdes qui appellent une anticipation de la part d'entreprises qui sont encore 57% à déclarer n'avoir pas mis en place de plan d'urgence.
Si la tendance actuelle est de laisser de plus en plus la main à l'intelligence artificielle pour contrecarrer les mauvaises décisions humaines, il semble qu'en la matière, nous ayons encore un rôle à jouer. Bonne nouvelle ou dernier écrin d'autonomie dans un océan d'automatisation des procédés, il ne s'agit pas de trancher mais bien de connaître les bons réflexes qui doivent protéger votre activité.

Les techniques les plus utilisées :

1. **La fraude au « faux fournisseur » :** terriblement perverse, cette fraude se joue en plusieurs temps. Au premier temps de la fraude, le fraudeur commence par identifier un de vos plus importants fournisseurs, le contacte et, se faisant passer pour votre comptable ou responsable des achats, demande l'intégralité des factures en cours. Au deuxième temps, c'est à votre tour d'être contacté. Signalant un changement de compte bancaire et renvoyant la totalité des factures alors obtenues, vous demande de régler votre dû. Au troisième temps, vous venez d'être cyber-escroqué. Ce qui est aussi désagréable d'être escroqué tout court, mais dans l'intimité de votre bureau.
2. **L'usurpation d'identité :** pillage de fichiers clients, vol d'informations et d'appel d'offres dans le cadre d'un concours … Les bonnes raisons sont nombreuses, les techniques aussi.
3. **Fraude aux faux banquiers, avocats ou commissaires aux comptes**

4. **Ransomware** : l'ouverture d'un mail malveillant, la transmission d'informations sur un site piraté et vous pouvez être contaminé par ce type de rançongiciel. Le principe est simple : il vous prive de toutes vos données et demande une rançon en échange d'une clé qui permettra de déchiffrer vos documents. Payer n'est bien entendu pas la solution.

Comment se prémunir face à ces attaques ? Quelques conseils pour vous.

Prévenir avant de guérir :

Le nerf de cette guerre virtuelle est la sacrosainte *data*. Il ne s'agit que d'elle et la possibilité de vous la substituer. La première étape est donc de vous offrir une cartographie exhaustive de votre écosystème digital : quelles sont les portes d'entrées possibles ? Qui gèrent les accès et possèdent des habilitations ?

Il convient également de répartir les rôles en interne pour qu'en cas d'attaque, chacun agisse au plus vite : contact avec les tiers concernés (assurances, avocats, police …), rassurer vos clients, couper le réseau internet …

Il vous faut également mettre en place des process de sauvegarde des données, automatisés et sécurisés. Cette mise en garde dépasse d'ailleurs largement le cadre de la cybercriminalité et offre un back-up salutaire en cas de défaillance de votre matériel, d'incendie, de dégâts des eaux etc … Votre stratégie de sauvegarde doit vous permettre de réduire au maximum la période de cessation d'activité, en reprenant quasiment là où vous aviez arrêté avant le sinistre.

Pour ce faire, plusieurs solutions s'offrent à vous, de la sauvegarde manuelle sur un disque dur externe à l'automatisation de sauvegardes instantanées sur des serveurs à distance, minimisant la perte de données.

Adopter les bonnes pratiques :

Si les verrous numériques doivent être adaptés à l'importance de la menace, il y a toutefois de bons réflexes qui peuvent s'avérer utiles :

- Choisir des mots de passe d'au moins 12 caractères, de types différents (majuscules, chiffres, caractères spéciaux…). Le nom de votre animal de compagnie et votre année de naissance n'est pas un mot de passe compliqué. Lsldv2l'aB ?mcd'1lm si.
- Ne pas modifier le contenu de votre site internet ou de vos réseaux sociaux professionnels depuis un smartphone. Privilégiez l'utilisation d'un poste unique et sécurisé.
- Mettre à jour très régulièrement vos outils : navigateurs internet, antivirus, bureautique … Un logiciel qui n'est pas à jour c'est une faille dans votre sécurité. Et les cyberpirates n'ont pas vraiment besoin que vous leur facilitiez la vie.
- Ne pas ouvrir de pièces jointes venant de destinataires inconnus

Que faire lorsque vous êtes l'objet d'une cyberattaque ?

- Stopper net la propagation : pour cela, il convient de couper immédiatement votre connexion internet. Plus vite vous réagissez, plus vite vous stoppez les dégâts. Tout ce qui compose votre univers informatique doit être déconnecté : ordinateurs, disques durs, terminaux … Attention toutefois à ne pas couper l'alimentation ! Vous risqueriez de supprimer les preuves de l'attaque, indispensable au dépôt de plainte.
- Neutraliser l'attaque : De retour dans le calme après une tempête qui vous aura vu débrancher à la hâte les câbles réseaux, il vous faut maintenant vous débarrassez du parasite numérique. Si vous n'êtes pas entouré d'experts capables de gérer la situation en interne, tournez-vous vers votre assureur. Entre bons conseils et procédures à suivre, il saura vous expliquer les gestes qui sauvent. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) peut également vous proposer une liste de prestataires disposant du label CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) qui vous aideront à définir l'origine de l'attaque afin de la circonscrire au mieux.

- Conserver les preuves : Lors du dépôt de plainte, il vous sera demandé une batterie de justificatifs que vous devrez être en mesure de fournir pour prouver l'attaque et déclencher les indemnisations : journal de connexions, captures réseaux, copie des disques durs des machins infectées au moment de la découverte de l'intrusion, échanges avec des tiers pendant l'attaque …
- Restaurer le système d'exploitation : Sans parler d'un remplacement de l'ensemble du matériel infecté, il faudra au minimum réinstaller le système d'exploitation, enrichi des correctifs de sécurité nécessaire avant de se reconnecter au réseau. Il vous faudra également modifier l'ensemble des mots de passe utilisés jusqu'alors.

L'accompagnement Cybersécurité de la MAF :
Pour anticiper les risques et mettre en place une protection efficace, notre assurance Cyber Sécurité vous couvre tout au long de votre cyber-existence :

- Restauration des données électroniques en cas d'attaque.
- Prise en charge des frais liés à une enquête administrative ou liés à une gestion de crise par des experts informatiques.
- Protection contre la cyber-extorsion (paiement d'une rançon en échange de la non-divulgation d'informations).
- Couverture pour vos possibles pertes d'exploitation consécutives à une interruption matérielle de votre réseau professionnel.

Notre contrat vous procure les garanties suivantes :

- Centre d'appel 24h/24 et 7j/7 pour organiser les premières actions d'urgence qui s'imposent suite à une cyber attaque.
- Accès à un réseau d'experts : conseil juridiques, experts informatiques et spécialistes de la communication.
- Une cotisation sur-mesure selon les montants de garantie souhaités.

Vous souhaitez que nos experts vous accompagnent dans la gestion et la protection de votre écosystème digital ? **Découvrez notre offre** et demandez nous de vous appeler pour échanger sur le sujet. Promis on le fera.

**enquête réalisée à l'occasion du troisième baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)*