Livre blanc

Cybersécurité : protégez votre activité et les données personnelles de vos clients

galian - smabtp

Sommaire

Introduction

Vol de données, menaces d'extorsion ou encore atteinte à la e-réputation… les risques cyber sont multiples.

Parmi les pays les plus exposés aux risques cyber, la France arrive en troisième position, derrière les États-Unis et la Russie.*

En 2018 déjà, la cybercriminalité faisait des ravages auprès des entreprises : 80 % d'entre elles avaient connu au moins une cyberattaque et 32 % plus de 10 !**

Selon les éléments fournis par Cybermalvaillance.gouv.fr***, les principales cyberattaques signalées par les professionnels en 2023 étaient :

- le piratage de compte (23,5 %),
- l'hameçonnage (21,2 %),
- le rançongiciel (16,6 %),
- le faux ordre de virement (10,2 %),
- la violation de données (8,7 %).

Pourquoi les entreprises sont-elles autant ciblées ? À cause de l'accélération de la transformation digitale, de l'absence de protection ou de politique de sécurité des systèmes informatiques, du manque de sensibilisation et de formation du personnel, de la démocratisation du télétravail… Les causes sont nombreuses.

Face à la multitude de cyberattaques et à la complexité du sujet, souscrire à une assurance cybersécurité est primordial.

Comment protéger votre agence des cybermenaces ? Comment sensibiliser et former vos collaborateurs aux risques cyber ? Quelles actions mettre en place pour sécuriser vos données personnelles et celles de vos clients ? GALIAN-SMABTP, l'assureur de référence des professionnels de l'immobilier, répond à toutes vos interrogations dans ce guide !

*Source : étude sur les violations de données personnelles à l'échelle mondiale depuis 2004 de Surfshark.
**Source : ministère de l'Intérieur et des Outre-mer.
***Source : Rapport d'activité 2023 – Au cœur de l'action cyber.

I. Pourquoi le secteur de l'immobilier est-il particulièrement exposé aux cyberattaques ?

Quelle que soit l'activité (transaction, gestion ou syndic), le secteur de l'immobilier est particulièrement exposé aux cyberattaques.

Pourquoi ? Parce qu'il implique des **données d'identité sensibles liées aux clients**, mais aussi aux partenaires (notaires, courtiers, banques, mandataires, etc.), ainsi que des **informations financières**.

Ces flux font des professionnels de l'immobilier des cibles de choix pour les cybercriminels.

La transformation digitale, le manque de formation et de sensibilisation des collaborateurs sont aussi des facteurs de risques.

1. Professionnels de l'immobilier : à quels risques êtes-vous exposés ?

Agent immobilier, administrateur de biens ou syndic, vous êtes exposés aux mêmes risques :

- vol de données,
- perte ou destruction de vos données clients,
- menaces d'extorsion,
- blocage complet du système informatique et/ou de celui de votre prestataire,
- atteinte à votre e-réputation,
- menaces à la suite d'erreurs humaines, etc.

Tous ces risques engendrent une perte de productivité jusqu'à l'impossibilité d'exercer votre activité professionnelle.

2. Quelles sont les cyberattaques les plus connues ?

La cybercriminalité ne cesse d'évoluer : les hackers sont de plus en plus ingénieux et les cyberattaques plus pernicieuses.

Les attaques les plus courantes sont notamment :

1. **Le phishing** : également appelée « hameçonnage », cette technique consiste à voler les données d'une entreprise ou d'un particulier afin de les revendre.
2. **Le ransomware** : connu également sous le nom de « rançongiciel », le ransomware est un type de logiciel qui bloque l'accès d'une entreprise à ses données. Le hacker demande ensuite une rançon en échange de la restitution de ces dernières.
3. **L'arnaque au président** : il s'agit ici d'une usurpation d'identité. Le pirate informatique va se faire passer pour une personne importante de l'entreprise (dirigeant, président, etc.) afin de demander à sa victime (un employé) d'effectuer un virement en urgence. L'argent est alors détourné vers un compte appartenant au hacker.
4. **Le déni de service** (ou déni de service distribué – DDoS) : cette cyberattaque paralyse l'ensemble du réseau informatique de l'entreprise. Il est alors inutilisable.
5. **Le malware** : ce logiciel malveillant est injecté dans le système informatique de l'entreprise, afin d'en perturber son fonctionnement et d'obtenir des informations confidentielles. Ce malware peut prendre la forme d'un virus informatique, d'un Cheval de Troie ou encore d'un spyware.
6. **Le téléchargement furtif** ou « Drive by download » : lorsque vous ne mettez pas à jour vos logiciels, vous risquez de subir ce type d'attaque. Ce logiciel malveillant s'insère dans les failles de sécurité des navigateurs web ou des systèmes d'exploitation non mis à jour.

Cette liste non exhaustive prouve que les cyberattaques peuvent prendre différentes formes et qu'une bonne protection cyber ne s'improvise pas !

BON À SAVOIR +

Le paiement de la rançon ne garantit pas la récupération de vos données. Même si cela était le cas, vos données pourraient être exfiltrées et revendues sur le « Dark Web », là où les cybercriminels font leur marché.

3. TPE, PME, grands groupes : qui est le plus touché ?

Vous pensez que votre agence est bien trop petite pour attirer les hackers ? Détrompez-vous !

Quelle que soit la taille de l'entreprise, tous les professionnels de l'immobilier – gestionnaires, transactionnaires et syndics de copropriétés – sont concernés.

Néanmoins, ce sont les plus petites entreprises qui sont les cibles privilégiées des hackers. Pourquoi ? Tout simplement parce qu'elles se pensent à l'abri des cyberattaques, alors qu'elles sont des cibles idéales car mal préparées et non dotées d'outils performants en cybersécurité.

PAROLE D'EXPERT

« Les cyberattaques réussies auprès des PME de moins de 50 salariés sont bien plus nombreuses que ce que l'on croit. Surtout par rançongiciel (cryptovirus). »

Philippe LAURIER, Chercheur à l'IRT SystemX (Institut de Recherche Technologique).

Résultat, selon le Rapport du Sénat du 10 juin 2021*, **60 % des PME ont fait faillite dans les 18 mois suivant une cyberattaque.**

Dans son panorama de la cybermenace 2022, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) indique que **les TPE, PME et ETI représentent 90 % des cyberattaques en 2022** et que 40 % d'entre elles ont subi une attaque par rançongiciel (ransomware).

Ainsi, les PME sont 9 fois plus touchées que les grands groupes par les risques cyber !

*Source : Rapport d'information n° 678 (2020-2021) du Sénat, déposé le 10 juin 2021.

II. 8 conseils pour protéger votre activité des cybermenaces

Pour protéger efficacement votre entreprise des cybermenaces, un certain nombre d'actions sont à mettre en place. Voici 8 conseils pour éviter les mauvaises surprises !

1. Sauvegarder quotidiennement vos données

Effectuez quotidiennement des sauvegardes de vos données. Vous pouvez les stocker sur des conteneurs numériques sécurisés.

Ainsi, en cas de vol de données, vous retrouverez votre dernière sauvegarde.

2. Mettre à jour vos logiciels dès que c'est nécessaire

Trop souvent, lorsque vous recevez une alerte de mise à jour à effectuer sur votre ordinateur, vous refusez de la lancer, de peur de perdre du temps dans votre planning déjà bien chargé !

Vous commettez une erreur : **ces mises à jour sont très importantes pour maintenir un bon niveau de protection de vos logiciels et de votre équipement informatique.**

Alors prenez 5 minutes pour les faire !

3. Utiliser un mot de passe complexe

On ne le dira jamais assez : avoir un mot de passe complexe est le b.a.-ba en matière d'informatique !

Oubliez les références personnelles : choisissez un mot de passe robuste contenant au moins 12 caractères, des chiffres, des caractères spéciaux, des majuscules et des minuscules.

Votre mot de passe doit être à utilisation unique ! Cela signifie qu'il ne doit pas être utilisé pour d'autres comptes.

Vous avez peur de ne pas vous en rappeler ? Pas de panique, il existe des gestionnaires de mots de passe, des conteneurs sécurisés ou coffres-forts numériques, conçus pour stocker les mots de passe de tous vos comptes ! Il en existe des gratuits, comme Keepass, qui est d'ailleurs recommandé par l'ANSSI.

Enfin, pensez à changer régulièrement votre mot de passe pour plus de sécurité.

4. Sensibiliser et former vos collaborateurs aux cybermenaces

Il est important de sensibiliser l'ensemble de vos collaborateurs, qu'ils soient salariés ou non, afin qu'ils puissent identifier les risques cyber et savoir comment réagir en cas d'attaque.

Cela passe par de la formation et par la mise en place d'une politique de sécurité, notamment en ce qui concerne le respect du RGPD (le règlement général sur la protection des données).

Veillez aussi à les sensibiliser quant au fait de ne pas utiliser leur ordinateur à des fins personnelles ou pour surfer sur les réseaux sociaux, potentiellement dangereux.

LE SAVIEZ-VOUS ?

Dans le cadre du règlement européen RGPD, entré en application le 25 mai 2018, tout professionnel a une obligation d'avertir son portefeuille clients, ainsi que la CNIL (Commission nationale de l'informatique et des libertés), dès lors qu'une usurpation de données est constatée.

5. Vérifier systématiquement l'identité de votre interlocuteur

Avant de transmettre des informations sensibles, assurez-vous de **bien vérifier l'identité de votre destinataire**. Pour l'envoi des documents, utilisez un canal sécurisé prévu à cet effet.

6. S'équiper d'outils dédiés à la cybersécurité

L'utilisation d'outils dédiés à la cybersécurité vient en complément des actions précédemment citées.

Ainsi, pensez à faire **installer un antivirus, un pare-feu**, etc., sur l'ensemble de votre équipement informatique.

Veillez aussi à ne pas utiliser les réseaux WI-FI publics.

7. Sécuriser votre espace de travail

Afin d'éviter l'usurpation d'identité ou le vol d'informations stratégiques, pensez aussi à **sécuriser votre espace de travail**.

Que ce soit en agence, chez un client ou chez vous, pensez à **verrouiller systématiquement votre ordinateur lorsque vous quittez votre poste de travail**.

En laissant votre écran déverrouillé, vous donnez accès aux informations de votre entreprise à n'importe qui. Une personne malveillante peut alors effectuer des actions en votre absence, via votre ordinateur, qui seront ensuite associées à votre compte et à votre identité.

Soyez vigilant !

8. Souscrire une cyber assurance

La meilleure solution pour vous prémunir contre les cyberattaques est de **souscrire à une assurance cyber.** Pourquoi ? Tout simplement parce que cette dernière va vous protéger efficacement contre tous les risques cyber et vous permettre de continuer votre activité.

En suivant ces préceptes, vous serez mieux armé face à la cybercriminalité.

Néanmoins, le risque zéro n'existe pas : même en adoptant toutes ces précautions d'usage, les hackers parviennent sans cesse à déjouer les mesures de sécurité mises en place.

Comment sensibiliser vos collaborateurs aux risques cyber ?

Le facteur humain est l'une des premières causes des cyberattaques. Arnaque au président, e-mail frauduleux… la plupart des attaques aboutissent grâce à l'intervention humaine.

Comment y remédier ? En formant régulièrement vos collaborateurs, mais pas seulement.

1. Élaborez une politique de sécurité

Vous devez également élaborer une politique de sécurité et la faire appliquer au sein de votre agence. Comment ? En mettant par exemple à disposition de vos équipes, un guide de la cybersécurité répertoriant toutes les bonnes pratiques. En partageant notre guide !

Vous devez avoir une stratégie de surveillance et de gestion des incidents informatiques au sein de votre structure, et ce, afin d'éviter la violation de vos données personnelles et celles de vos clients.

2. Faites de la veille

Parce que les cybermenaces sont en perpétuelle évolution, avec des attaques de plus en plus perfectionnées, il est indispensable de tenir vos collaborateurs informés régulièrement des dernières tendances en matière de cybersécurité.

Pour cela, vous pouvez mettre en place une veille, notamment pour le secteur de l'immobilier, et consulter régulièrement les sites gouvernementaux comme l'ANSSI, le site cybermalveillance.gouv.fr ou le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse).

3. Systématisez l'utilisation d'outils technologiques par vos équipes

Il est primordial de déployer une stratégie comprenant des outils ou dispositifs visant à protéger votre réseau informatique contre toute tentative d'intrusion. Pare-feu, chiffrement des données, authentification à double facteur, antivirus, VPN… sont autant de bonnes pratiques à mettre en place auprès de vos collaborateurs.

III. Zoom sur l'assurance Cybersécurité GALIAN-SMABTP

Mettre en place une politique de cybersécurité efficace repose sur de nombreux paramètres et une vigilance de tous les instants. La meilleure solution pour lutter contre la cybercriminalité demeure de souscrire à une assurance cybersécurité.

Souscrire à l'assurance Cybersécurité de GALIAN-SMABTP, c'est bénéficier :

1. **D'une protection complète contre les risques liés à la cybercriminalité** portant atteinte à la sécurité du réseau informatique de votre agence.
2. **D'une hotline de spécialistes en incidents cyber** présents de la découverte de la cyberattaque à sa réparation.
3. **D'un accompagnement juridique** en cas de recours devant les tribunaux, en cas de mise en cause de votre Responsabilité Civile Professionnelle (RCP) quant à l'utilisation des données personnelles de vos clients.
4. **D'une assistance financière** afin de régler d'éventuelles indemnités à vos clients ou à des tiers.
5. **D'une prise en charge des impacts financiers liés à votre e-réputation.** En cas d'atteinte à votre réputation en ligne, GALIAN-SMABTP prend en charge les frais de notification obligatoire et de communication à vos clients en cas de fuite de données personnelles.
6. **D'une prise en charge des frais liés à votre reprise d'activité** comme les frais de transfert vers un autre prestataire d'externalisation, les frais de monitoring et de surveillance, les frais liés à la récupération de vos données, etc.
7. **D'une garantie perte d'exploitation** afin de préserver votre chiffre d'affaires en cas de cyberattaque.
8. **D'une offre pensée pour les professionnels de l'immobilier,** qu'ils exercent une activité de transaction, de gestion ou de syndic.

EXEMPLE DE VOL ET DE PERTE DE DONNÉES EN TRANSACTION

Une agence immobilière, composée de trois salariés, est victime d'une intrusion malveillante dans ses secteurs de sauvegarde, ce qui a engendré le vol des données personnelles de ses clients.

Avec une assurance cyber : l'assureur a pu accompagner rapidement l'agence immobilière en lui mettant à disposition un conseiller spécialisé et un consultant en communication de crise pour limiter les risques d'image. L'assureur a pris en charge 35 000 euros de frais pour ce sinistre qui correspondent aux garanties de mesure d'urgence et de gestion de crise. L'assureur a notifié auprès de la CNIL, l'usurpation des données et a pris en charge les 170 000 euros de frais d'information des clients de l'agence immobilière.

EXEMPLE D'USURPATION D'IDENTITÉ EN GESTION

Un individu se fait passer pour un conseiller de la banque et demande au comptable de l'agence de revalider les virements s'adressant à des propriétaires passés quelques heures plus tôt.

Avec une assurance cyber : le sinistre, après expertise de l'assureur, est évalué à 39 691 euros. Le client perçoit l'intégralité de la somme réclamée conformément aux conditions de son contrat.

EXEMPLE DE CYBER-EXTORSION EN SYNDIC

Un syndic de copropriété a reçu un e-mail de l'un de ses fournisseurs réclamant le règlement urgent d'une facture. Il s'agit en réalité d'un faux message et la pièce jointe est un ransomware qui crypte un grand nombre de données du système informatique de l'entreprise, rendant ces dernières totalement inaccessibles. Le pirate informatique réclame une rançon pour débloquer les données. Le syndic de copropriété appelle la cellule de crise. Le coordinateur de la cellule l'oriente vers un expert, afin qu'il puisse analyser le problème et déterminer si le cryptage peut être ou non facilement défait.

Avec une assurance cyber : l'assureur a pris en charge les frais de l'expert, les frais de reconstitution des données, ainsi que la perte d'exploitation subie par l'entreprise pendant la durée du blocage de son activité, pour un montant de 60 000 euros.

Que couvre l'assurance Cybersécurité de GALIAN-SMABTP ?

L'assurance Cybersécurité GALIAN-SMABTP comprend plusieurs plafonds annuels de garanties, avec un tarif adapté à vos besoins, forfaitaire ou sur-mesure.

Assistance et gestion de crise

- Mise à disposition d'une hotline dédiée accessible 24h/24 et 7j/7.
- Mesure d'urgence (sans franchise).
- Conseils donnés par une équipe d'experts en cybersécurité pour diagnostiquer, éradiquer la menace et aider à restaurer le système d'information (SI) à partir des sauvegardes.
- Restauration des données et du SI, dont les données personnelles et confidentielles.
- Atteinte à la réputation et aux relations publiques avec la mise en place de stratégies de communication adaptées.
- Accompagnement en termes de dépôts de plainte et/ou de signalement de l'incident, appui d'un expert informatique et d'un conseiller juridique spécialisé en gestion de crise.

Responsabilité civile

- Atteinte aux données personnelles.
- Atteinte aux données confidentielles.
- Manquement à l'obligation de notification.
- Externalisation et sous-traitance.
- Atteinte à la sécurité du réseau.
- Garantie média et publication numérique dommageable.
- Frais d'urgence (sans franchise).

BON À SAVOIR +

Les garanties de votre assurance Cybersécurité GALIAN-SMABTP se déclenchent dès votre appel à la plateforme d'assistance.

Selon les garanties choisies, une franchise peut s'appliquer (voir les conditions particulières de votre contrat).

Dommages et frais

- Cyber-extorsion ou demande de rançon (sans franchise).
- Perte d'exploitation (franchise de 12 h ou de 24 h si défaillance du système d'information).
- Frais de transfert vers un autre prestataire d'externalisation.
- Frais de notification et de communication.
- Frais de monitoring et de surveillance.
- Frais de surconsommation téléphonique.
- Pertes pécuniaires liées à un cyber-détournement de fonds.

GALIAN-SMABTP, l'assureur de référence des professionnels de l'immobilier

GALIAN-SMABTP, avec **60 ans d'expérience** et près de **12 000 clients-sociétaires**, a été créé par et pour les professionnels de l'immobilier.

GALIAN-SMABTP a pour mission d'accompagner les agents immobiliers, les administrateurs de biens et les syndics de copropriétés, mais aussi leurs clients, et de répondre à l'ensemble de leurs besoins.

Pour cela, **GALIAN-SMABTP** propose un accompagnement sur-mesure, de la souscription au règlement des sinistres, ainsi qu'une offre de produits :

Pour les professionnels de l'immobilier :

- Garantie Financière (GF)
- Responsabilité Civile Professionnelle (RCP)
- Protection Juridique (PJ)
- Complémentaire Santé et Prévoyance pour les TNS
- Complémentaire Santé et Prévoyance pour vos salariés
- Assurance Cybersécurité
- Assurance Multirisque Bureaux

Pour leurs clients :

- Garantie des Loyers Impayés (GLI)
- Assurance Multirisque du Propriétaire Non-Occupant (PNO)
- Protection Juridique des Copropriétés
- Assurance Multirisque Habitation
- Multirisque Copropriété
- DO Syndic

GALIAN-SMABTP met aussi à la disposition de ses clients-sociétaires, des services adaptés à leurs activités :

- Audit de la comptabilité mandant
- Registre LCB/FT
- Bibliothèque juridique numérique
- Service agrément GLI, etc.

Vous souhaitez protéger les données de votre entreprise et celles de vos clients ?

Prenez contact dès à présent avec un conseiller GALIAN-SMABTP !

Contacter un conseiller

galian - smabtp