Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

À LA UNE

Par Véronique Méot

Protégez-v ous !

Tandis que le marché de la cybersécurité n'est pas encore mature, les risques d'attaques augmentent, encouragés par la multiplication des écrans connectés et des usages. La question n'est plus de savoir si une PME sera ciblée par un acte de cybermalveillance, mais quand ? D'où la nécessité de mettre en œuvre une stratégie dédiée, mêlant audit, sensibilisation et bonnes pratiques.

est pas encore mature, les risques multiplication des écrans connectés voir si une PME sera ciblée par un ù la nécessité de mettre en œuvre sation et bonnes pratiques.

C'est la préoccupation du moment. La 10e édition du Forum international de cybersécurité vient de se dérouler à Lille les 23 et 24 janvier. De son côté, l'État envisage d'engager 1,6 million d'euros pour sa cyberdéfense. Sans parler des cyberattaques retentissantes, les virus WannaCry et NotPetya, qui ont paralysé des centaines de milliers d'ordinateurs et frappé des milliers d'entreprises au printemps 2017. La cybersécurité s'invite dans l'actualité parmi les sujets sensibles pour les entreprises. *«La majorité des attaques, non médiatisable, passe sous silence et est judiciairement invisible, car elle ne justifie pas un dépôt de plainte»*, observe Philippe Laurier, chercheur et auteur d'une étude sur les cyberattaques menée par l'Institut de recherche technologique SystemX.

LES PME prises pour cible

Les PME ne sont pas épargnées et semblent aussi exposées que les grandes entreprises, d'autant qu'elles sont plus vulnérables. *«Il faut aller sur le terrain, en immersion, pour mesurer le décalage entre ce que l'on croit savoir et la réalité»*, regrette Philippe Laurier. Selon les chercheurs de SystemX, les attaques seraient plus nombreuses que ce que les études diligentées par les prestataires informatiques indiquent. Mais elles coûteraient moins cher à leurs victimes. D'ailleurs, la question n'est plus de savoir si une entreprise va être ciblée, mais quand ? *«Les PME sont considérées comme des chevaux de Troie offrant un accès à des donneurs d'ordre plus importants. Dans la région de Toulouse, par exemple, nous avons vu des PME se faire attaquer parce qu'elles travaillent pour des grandes entreprises des secteurs aéronautique ou pharmaceutique»*, affirme Jean-Michel Denys, membre du groupe de travail audit informatique à la Compagnie régionale des commissaires aux comptes (CRCC) de Paris. Dans ce cas, les cyberattaques relèvent de l'espionnage industriel. Et la pression monte d'un cran. *«Je connais des PME qui ont perdu des contrats parce qu'elles ne savaient pas répondre aux exigences de leur donneur d'ordre en matière de cybersécurité»*, ajoute Philippe Trouchaud, expert en cybersécurité chez PwC. Plusieurs types d'attaques font des ravages : l'hameçonnage - ou phishing - est l'un des plus répandus. Il vise à obtenir les données financières ou les identifiants de connexion du destinataire d'un e-mail, voire ses droits d'accès au réseau de l'entreprise afin de s'y infiltrer. En recrudescence, le rançongiciel consiste à envoyer à la victime un logiciel malveillant qui chiffre ses données puis à lui demander une rançon - à payer en bitcoin - en échange du mot de passe de déchiffrement. *"Nous conseillons expressément aux entreprises de ne pas payer la rançon ni de faire confiance à une personne malveillante"*, glisse Luis Delabarre, expert en cybersécurité, représentant de Malwarebytes en France. Peu de PME disposent de portefeuille de bitcoin, ce qui limite leur capacité ➲

Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

de paiement. Mais il n'empêche, pas question de céder ! D'autant que les fameuses clés de déchiffrement ne sont pas toujours délivrées par les hackers. La fraude au président est également fréquente et peut être évitée par une plus extrême vigilance. Il s'agit d'une arnaque consistant à convaincre un collaborateur d'effectuer un virement à un tiers sur un prétendu ordre du dirigeant.

Les pratiques préventives

Dans les entreprises, l'attention de tous est requise. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié un *«guide de l'hygiène informatique»* contenant une quarantaine de mesures de prévention, ainsi que des conseils de bon sens pour limiter les risques d'exposition. Pour résumer, trois grands axes prévalent. Tout d'abord, au cœur du système informatique, la mise en place de pare-feu et antivirus, ainsi que la gestion des mises à jour des logiciels et des sauvegardes sont obligatoires. Ensuite, au niveau managérial, la formation et la sensibilisation des équipes doivent être une priorité. Enfin, il faut mettre en place des procédures claires au sein de l'entreprise : restriction des accès aux données sensibles (et différenciation administrateurs / utilisateurs), gestion des droits (en fonction des arrivées, départs, changements de poste des collaborateurs), supervision et contrôle des mises à jour des logiciels et des systèmes de sécurité, mode opératoire en cas de cyberattaque, etc. Les cabinets d'audit et d'expertise comptable proposent des diagnostics pour identifier les risques propres à l'entreprise. Victime de plusieurs attaques, dont récemment un ransomware qui lui a spolié la moitié de ses données, Sébastien de Wulf, gérant de la société Big Bennes, une PME de 70 salariés, a confié ce diagnostic au cabinet d'expertise comptable Fideliance. *« Partenaire de proximité, le cabinet me paraissait plus à même d'évaluer la situation que mon prestataire informatique, qui aurait été juge et partie»*, témoigne ce dirigeant dont la société a réalisé 22 millions

Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

d'euros de chiffre d'affaires l'année dernière. La mission s'est essentiellement axée sur la mise en place de procédures qui faisaient défaut à l'organisation, plutôt bien protégée. « *J'ai mis en place des tests de conformité notamment pour la vérification des sauvegardes, ainsi que des tests de restauration des données* », précise Christian Gabenesch, ingénieur spécialisé en sécurité informatique chez Fideliance. Car dans les systèmes informatiques, les failles apparaissent souvent par manque de vigilance. D'où l'importance du volet managérial et des procédures internes. Les collaborateurs doivent appliquer des règles de bon sens comme renforcer les accès aux données sensibles, privilégier l'authentification forte (un mot de passe et un numéro de téléphone pour recevoir un code SMS, une carte à puce et une empreinte biométrique...), utiliser un filtre de confidentialité sur les écrans mobiles, donner l'alerte en cas de comportements anormaux, etc. Bref, la vigilance doit être constante.

Souscrire une assurance

Face à la gravité du risque - une PME attaquée peut voir son activité s'arrêter net - une protection supplémentaire consiste à contracter une assurance. Plusieurs offres sont apparues sur le marché, critiquées par l'étude de SystemX, l'organisme considérant qu'elles s'attachent à répondre à des besoins secondaires. Mais il semble qu'elles évoluent : « *nous proposons de multiples garanties couvrant les impacts qu'une cyberattaque peut provoquer, du financement des frais liés à la gestion de crise (recours à un expert et à un avocat) à la garantie perte d'exploitation* », explique Dominique Jeune, expert en cybersécurité chez MMA Covea. Investir entre 1 000 et 4 000 euros environ permet de s'assurer une garantie dont le montant peut atteindre plusieurs centaines de milliers d'euros. « *Comme nous n'assurons pas un particulier contre le vol s'il ne verrouille pas son habitation, nous exigeons des entreprises un niveau minimum de prévention* », souligne l'expert.

Chef d'entreprise
LE KIT PRATIQUE DU DIRIGEANT DE PME

PAYS : France
PAGE(S) :1
SURFACE :320 %
PERIODICITE : Bimestriel

DIFFUSION :(70000)
JOURNALISTE : Veronique Meot

► **21 février 2018**

Une offre à construire

« Les menaces augmentent de plus de 70 % par an, quand le chiffre d'affaires lié à la cybersécurité ne progresse que de 9 % par an. Sa croissance est ralentie par le manque de ressources », constate Jean-Paul Alibert, président du comité cybersécurité au Syntec Numérique. La question des ressources se pose davantage pour les PME. *«Elles utilisent des méthodes dépassées et inadaptées face aux risques actuels»*, estime Hervé Dhelin, directeur marketing d'Efficient IP. *«Le Syntec Numérique travaille à l'ouverture, dès septembre, d'une formation courte afin de permettre aux informaticiens des PME de mieux appréhender les risques»*, annonce Jean-Paul Alibert. Le secteur de la cybersécurité manque d'outils et de compétences. Ce marché souffre *«d'une hétérogénéité excessive des compétences et d'une faible transparence sur le niveau réel de chaque prestataire»*. Que faire ? *« Nous recommandons aux PME qui ne peuvent pas intégrer les ressources en interne de faire appel à des fournisseurs de solutions SaaS, qui les déchargent de la gestion des outils»*, répond Jean-Paul Alibert. La plateforme Cybermalveillance.gouv.fr, en ligne depuis la mi-octobre 2017 via le GIP Acyma, dispositif d'assistance aux victimes, répertorie des prestataires spécialisés. *« Face à une attaque, nous fournissons une première réponse par les "fiches réflexes" à disposition afin d'aiguiller les victimes. Nous référençons aussi des prestataires qui ne sont pas pour autant qualifiés, mais qui se sont engagés via la signature d'une charte »*, précise Jérôme Notin, dg du dispositif national d'assistance aux victimes de cybermalveillance. De son côté, l'ANSSI publie des listes de prestataires dans plusieurs spécialités : détection des incidents de sécurité (PDIS), réponse aux incidents, audit des systèmes d'informations, etc. Ils répondent aux exigences de l'agence mais pratiquent, selon Jérôme Notin, *« des tarifs peu accessibles aux PME »*. Note d'optimisme, les observateurs pensent que le marché va se structurer dans les mois à venir, s'enrichir de solutions venues de l'intelligence artificielle et proposer des tarifs plus adéquats... ouvrant la voie à une meilleure résistance des PME. @Chef_Entreprise