La cybersécurité des PME, nouvel eldorado des assureurs

Avec la numérisation, de plus en plus d'activités sont exposées au piratage informatique. Si les grandes entreprises sont presque toutes couvertes pour ces risques, les PME restent à la traîne. Les assureurs redoublent d'efforts pour les convaincre.

En septembre 2017, lorsqu'il se rend dans sa PME à Clermont-Ferrand, André Thomas découvre tous ses ordinateurs paralysés par un ransomware. Le pirate lui demande 3000 euros qu'il refuse de payer. Toutes ses données perdues, l'entrepreneur doit mettre la clé sous la porte. Une mésaventure qui illustre le danger croissant auquel sont exposées nos 138 000 PME françaises.

Ransomware, arnaques par phishing, piratage d'une base de données stockée dans le cloud ou d'une caméra de surveillance… La numérisation des entreprises les expose à des risques croissants. En France, huit PME sur dix auraient déjà été touchées par une cyberattaque, d'après la firme Tehtris. Avec des conséquences financières souvent désastreuses : blocage des activités, atteinte à la réputation de l'entreprise, perte de clientèle et de chiffre d'affaires, perte de la base de données client, atteinte à la propriété intellectuelle, frais juridiques… Les dégâts se chiffrent à 240 000 euros en moyenne pour une PME, et une sur quatre peut même disparaître suite à un piratage.

Parallèlement, l'environnement législatif se fait de plus en plus contraignant.

La nouvelle règlementation européenne sur la protection des données personnelles (RGPD), qui entrera en vigueur en mai, expose les entreprises à de nouvelles menaces juridiques et à des amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires.

Seules 14% des PME ont souscrit une assurance cyber

Pourtant, seules 14% des petites entreprises disposent d'une assurance spécifique contre les cyberattaques, d'après une étude PwC. Alors que les grandes entreprises sont quasiment toutes couvertes, nos PME semblent elles encore inconscientes du danger : 51% estiment que « *les risques d'exposition trop faibles pour justifier de s'assurer* » et 39% d'entres elles n'ont pas souscrit car « *cela ne leur est pas venu à l'esprit* », d'après une autre étude de PwC.

Ce retard à l'allumage ne tient pas uniquement à un problème de demande. Selon un rapport du Club de juristes intitulé « Assurer le Risque cyber », il résulte également d'une offre inadaptée de la part de assureurs. Sur ce marché encore immature, les statistiques sont rares et l'expertise technique pour évaluer la vulnérabilité des entreprises est encore insuffisante, met-il en lumière. D'autant plus que les clients sont réticents à partager des informations confidentielles et stratégiques avec leur assureur, qui lui seraient pourtant bien utiles pour apprécier le risque et indemniser au mieux après un sinistre. D'où un «manque de corrélation entre les primes et le risque» aboutissant à des offres mal calibrées.

Les offres spécifiques en plein boom

Il n'empêche que le marché est en phase d'accélération. « *Nous avons doublé notre portefeuille de clients en 2017 et nous prévoyons de doubler encore ce chiffre sur les six premiers mois de 2018* », se félicite Laurence Lemerle, directrice des risques cyber chez Axa. L'assureur, qui assure déjà un tiers des PME françaises, propose une offre spécifique à destination de ces entreprises. Generali a emboité le pas en 2017 et explique vouloir « multiplier par six ou huit » son portefeuille en 2018. De nombreux assureurs étrangers se positionnent également avec des offres à destination des PME : Hiscox, Zurich, ACE, Beazley, QBE…

Des prestations additionnelles pour

marquer sa différence

Après une évaluation des risques avec un questionnaire (type de sauvegarde, présence d'un pare-feu ou antivirus, actions de sensibilisation des salariés…), un contrat sur mesure est établi. Le coût de la prime reste relativement modeste (autour de 1000 euros chez Generali), mais elle vient s'ajouter à toutes les dépenses de sécurité informatique que la PME doit déjà engager. Pour convaincre, les assureurs tentent donc de se démarquer avec des services additionnels. « C*e qui différencie un assureur d'un autre, ce n'est pas la protection financière et les garanties mises en place, qui sont semblables, c'est la valeur ajoutée du prestataire spécialisé* », explique le courtier spécialisé Assurance cybercriminalité. Certains contrats incluent ainsi des conseils juridiques, une stratégie de communication et de relations presse après une attaque, un diagnostic technique ou des audits de sécurité : le contrat de QBE France comprend par exemple des tests d'intrusion dans les systèmes d'information.

Pour ces prestations, les assureurs s'allient les services de spécialistes de la cybersécurité. Generali s'est par exemple associé à Europ Assistance et Ineo, la filiale d'Engie pour les territoires connectés. Axa travaille avec une filiale d'Airbus et Yogosha, une startup française hébergée à Station F et spécialisée dans le « bug bounty » (chasse aux failles d'un système informatique). « *L'évaluation du risque reste cependant beaucoup plus artisanale que pour des catastrophes naturelles, où l'on dispose d'un historique sur une longue période», reconnaît Laurence Lemerle. «Les cyber-risques évoluent à chaque minute* », renchérit Denis Kessler, le PDG du réassureur Scor.

Le spectre d'une paralysie mondiale

Si la cybersécurité est une énorme opportunité pour les assureurs, elle représente aussi une grosse menace potentielle : celle d'une attaque massive qui toucherait un très grand nombre d'entreprises. « *Imaginons que tout d'un coup, les systèmes de paiement du monde entier tombent en rade en même temps* », s'inquiète Denis Kessler. « *Dans 15 ans, le risque cyber dépassera celui de toutes les catastrophes naturelles réunies* », avance-t-il. Un véritable « *désastre* » auquel le secteur n'est pas encore préparé. « *Il va falloir inventer des formes de réassurance plus sophistiquées* », reconnaît Didier Parsoire, qui gère le risque cyber chez le réassureur.

En septembre 2017, lorsqu'il se rend dans sa PME à Clermont-Ferrand, André Thomas découvre tous ses ordinateurs paralysés par un ransomware. Le pirate lui demande 3000 euros qu'il refuse de payer. Toutes ses données perdues, l'entrepreneur doit mettre la clé sous la porte. Une mésaventure qui illustre le

danger croissant auquel sont exposées nos 138 000 PME françaises.

Ransomware, arnaques par phishing, piratage d'une base de données stockée dans le cloud ou d'une caméra de surveillance… La numérisation des entreprises expose les entreprises à des risques croissants. En France, huit PME sur dix auraient déjà été touchées par une cyberattaque d'après la firme Tehtris. Avec des conséquences financières souvent désastreuses : blocage des activités, atteinte à la réputation de l'entreprise, perte de clientèle et de chiffre d'affaires, perte de la base de données client, atteinte à la propriété intellectuelle, frais juridiques… Les dégâts se chiffrent à 240 000 euros en moyenne pour une PME, et une sur quatre peut même disparaître suite à un piratage.

Parallèlement, l'environnement législatif se fait de plus en plus contraignant. La nouvelle règlementation européenne sur la protection des données personnelles (RGPD), qui entrera en vigueur en mai, expose les entreprises à de nouvelles menaces juridiques et à des amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires.

Seules 14% des PME ont souscrit une assurance cyber

Pourtant, seules 14% des petites entreprises disposent d'une assurance spécifique contre les cyberattaques, d'après une étude PwC. Alors que les grandes entreprises sont quasiment toutes couvertes, nos PME semblent elles encore inconscientes du danger : 51% estiment que «les risques d'exposition trop faibles pour justifier de s'assurer» et 39% d'entres elles n'ont pas souscrit car «cela ne leur est pas venu à l'esprit», d'après une autre étude de PwC.

Ce retard à l'allumage ne tient pas uniquement à un problème de demande. Selon un rapport du Club de juristes intitulé «Assurer le Risque cyber», il résulte également d'une offre inadaptée de la part de assureurs. Sur ce marché encore immature, les statistiques sont rares et l'expertise technique pour évaluer la vulnérabilité des entreprises est encore insuffisante, met-il en lumière. D'autant plus que les clients sont réticents à partager des informations confidentielles et stratégiques avec leur assureur, qui lui seraient pourtant bien utiles pour apprécier le risque et indemniser au mieux après un sinistre. D'où un «manque de corrélation entre les primes et le risque» aboutissant à des offres mal calibrées.

Les offres spécifiques en plein boom

Il n'empêche que le marché est en phase d'accélération. «Nous avons doublé notre portefeuille de clients en 2017 et nous prévoyons de doubler encore ce chiffre sur les six premiers mois de 2018», se félicite Laurence Lemerle, directrice des risques cyber chez Axa. L'assureur, qui assure déjà un tiers des PME françaises, propose une offre spécifique à destination de ces entreprises.

Generali a emboité le pas en 2017 et explique vouloir «multiplier par six ou huit» son portefeuille en 2018. De nombreux assureurs étrangers se positionnent également avec des offres à destination des PME : Hiscox, Zurich, ACE, Beazley, QBE…

Des prestations additionnelles pour marquer sa différence

Après une évaluation des risques avec un questionnaire (type de sauvegarde, présence d'un pare-feu ou antivirus, actions de sensibilisation des salariés…), un contrat sur mesure est établi. Le coût de la prime reste relativement modeste (autour de 1000 euros chez Generali), mais elle vient s'ajouter à toutes les dépenses de sécurité informatique que la PME doit déjà engager. Pour convaincre, les assureurs tentent donc de se démarquer avec des services additionnels. «Ce qui différencie un assureur d'un autre, ce n'est pas la protection financière et les garanties mises en place, qui sont semblables, c'est la valeur ajoutée du prestataire spécialisé», explique le courtier spécialisé Assurance cybercriminalité. Certains contrats incluent ainsi des conseils juridiques, une stratégie de communication et de relations presse après une attaque, un diagnostic technique ou des audits de sécurité : le contrat de QBE France comprend par exemple des tests d'intrusion dans les systèmes d'information.

Pour ces prestations, les assureurs s'allient les services de spécialistes de la cybersécurité. Generali s'est par exemple associé à Europ Assistance et Ineo, la filiale d'Engie pour les territoires connectés. Axa travaille avec une filiale d'Airbus et Yogosha, une startup française hébergée à la station F et spécialisée dans le «bug bounty» (chasse aux failles d'un système informatique). «L'évaluation du risque reste cependant beaucoup plus artisanale que pour des catastrophes naturelles, où l'on dispose d'un historique sur une longue période», reconnaît Laurence Lemerle. «Les cyber-risques évoluent à chaque minute», renchérit Denis Kessler, le PDG du réassureur Scor.

Le spectre d'une paralysie mondiale

Si la cybersécurité est une énorme opportunité pour les assureurs, elle représente aussi une grosse menace potentielle : celle d'une attaque massive qui toucherait un très grand nombre d'entreprises. «Imaginons que tout d'un coup, tous les systèmes de paiement du monde entier tombent en rade en même temps», s'inquiète Denis Kessler. «Dans 15 ans, le risque cyber dépassera celui de toutes les catastrophes naturelles réunies», avance-t-il. Un véritable «désastre» auquel le secteur n'est pas encore préparé. «Il va falloir inventer des formes de réassurance plus sophistiquées», reconnaît Didier Parsoire, qui gère le risque cyber chez le réassureur.