«La cybersécurité nous concerne tous, sans exception!»

La cybersécurité est l'une des principales menaces pour les entreprises, les organisations et les individus.

INTERVIEW **ANDREA TARANTINI**

Aujourd'hui, la transformation digitale et les progrès technologiques vont de pair avec les risques de cyberattaques en constante augmentation qui mettent à mal les entreprises et les organisations suisses. Toute société dépend désormais d'un système d'information et d'outils qui lui permettent de communiquer, de stocker, manipuler et échanger tous types de données. Cette dépendance est à la base de vulnérabilités importantes qui concernent non seulement les entreprises et l'économie mais aussi l'État et la société tout entière.

Fasciné par l'évolution du monde économique ainsi que celui de la recherche et de l'innovation, Béat Kunz, économiste d'entreprise, s'intéresse depuis 2017 au développement du monde digital, de la cybersécurité et de la cyberdéfense en Suisse. Ainsi, avec quelques associés, il crée le Forum national dédié à la cybersécurité, les Swiss Cyber Security Days qui réunit les principaux acteurs nationaux et internationaux du domaine. Dans l'interview qui suit, l'expertise de Béat Kunz ainsi que les connaissances approfondies de Paul Such, CEO de Hacknowledge SA, une des sociétés suisses les plus performantes dans le domaine de la cybersécurité, nous aident à comprendre les enjeux et les défis actuels en termes de cybersécurité.

Pourquoi la cybersécurité devrait-elle être une priorité aujourd'hui?
Paul Such: Du fleuriste au banquier en passant par le secrétaire et le gouvernement, toutes les sociétés, indépendamment de leur secteur d'activité, sont aujourd'hui dépendantes d'un système d'information fonctionnel. Au quotidien, toutes les entreprises et les organisations gèrent des factures, des commandes, une comptabilité et des dossiers clients par exemple. De nos jours, les progrès technologiques sont proportionnels aux risques en termes de cyberattaques. Aujourd'hui, nous ne pourrions pas travailler sans informatique, c'est pourquoi nous ne pouvons éviter de soulever le thème de la cybersécurité qui doit être une priorité.

Aujourd'hui, connaît-t-on le taux actuel d'entreprises et d'organisations qui dédient assez d'attention et de ressources à la sécurité de leur technologie et aux mises à jour de leurs systèmes?
PS: Malheureusement, nous ne disposons pas (encore) de chiffres précis à ce sujet en Suisse. Globalement, les problématiques de cybersécurité sont désormais un sujet de préoccupation pour les directions et les conseils d'administration et les budgets alloués à la sécurité augmentent. Le problème, c'est que la sécurité est un sujet transverse à la société qui concerne toutes les entreprises et organisations qui disposent d'un système d'information. Indépendamment du secteur d'activité, on ne devient pas «plus sûr» en ajoutant une solution magique ou en embauchant plus de monde. Aujourd'hui, on sait que, en moyenne, les sociétés mettent toujours plus de deux mois à se rendre compte qu'elles ont eu un incident de sécurité. Cela nous fait donc comprendre que beaucoup d'efforts sont encore nécessaires. Augmenter son niveau de sécurité, cela implique une certaine cohérence, de la rigueur et de la méthode. Il s'agit d'un effort permanent!

La confidentialité des données devient une priorité pour un plus grand nombre d'acteurs, indépendamment de leur secteur d'activité. Quelles sont les conséquences de cela?
PS: Certaines contraintes régulatrices ou légales (nouvelle LPD, GDPR, directives FINMA) ont poussé de nombreuses sociétés à prendre enfin au sérieux les aspects liés à la confidentialité des données. Cependant, et par expérience, quand un projet est uniquement conduit pour répondre à une exigence légale ou de conformité, il s'avère souvent techniquement un échec.

En 2020, quels sont les principaux challenges en termes de cybersécurité?
PS: Cette année est un peu particulière. À cause du Covid-19, de nombreuses sociétés ont dû s'organiser pour permettre le travail à distance. Elles ont notamment dû fournir des ordinateurs portables aux employés, permettre des connexions distantes et gérer les problématiques de dimensionnement par exemple. Cela a évidemment fait surgir de nombreuses contraintes en termes de sécurité, particulièrement pour les entreprises au sein desquelles ces problématiques n'avaient pas été anticipées.

Quels sont les principaux types de cyberattaques?
PS: Le sujet est vaste et les types de cyberattaques sont nombreux et en constante évolution. Il existe par exemple des attaques par déni de service (DoS) ou par déni de service distribué (DDoS), ces attaques entraînent l'effondrement du système d'information d'une entreprise qui devient inopérant suite à un excès d'informations inutiles provenant d'un réseau d'ordinateurs contrôlés par le pirate. Un autre type d'attaque est l'interception de données, l'Homme du milieu (MiTM). De nombreuses cyberattaques ciblent les utilisateurs. C'est notamment le cas de l'ingénierie sociale, de l'hameçonnage (phishing) et du harponnage (spear phishing). Souvent, les entreprises doivent aussi faire face aux attaques via un code malveillant (virus ou cheval de Troie, par exemple), aux attaques web et leurs variantes (Injection SQL, XSS), aux attaques sur les mots de passe et celles venant de gouvernements et englobant souvent les attaques déjà mentionnées.

Quelle est la différence entre menace, vulnérabilité et risque?
PS: Ces trois notions sont très proches, mais elles méritent d'être clairement distinguées. Une menace est un danger comme un accident, une erreur, une malveillance passive qui porte sur la confidentialité, une malveillance active qui concerne le contenu de l'information ou le comportement des systèmes de traitement, qui existe dans l'environnement d'un système indépendamment de celui-ci. En revanche, une vulnérabilité est une faiblesse du système, comme un bug ou un problème de configuration, qui le rend sensible à une menace. En général, les vulnérabilités les plus courantes sont celles liées à l'humain (social engineering), autrement, les bugs et les problèmes de configuration et relatifs à un correctif manquant sont également très répandus. Enfin, un risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système.

Et quelles sont les principales mesures que doivent prendre les entreprises?
PS: Il est essentiel que toutes les entreprises mettent en place le minimum technique comme des contrôles d'accès, des mots de passe forts, une authentification à deux facteurs, une gestion adaptée des vulnérabilités. Ensuite, il faut gérer la sécurité comme quelque chose de transverse à l'entreprise. D'autres mesures importantes concernent l'évitement de silos et la responsabilisation des utilisateurs.

Quelles sont les questions qu'une entreprise ou une organisation devrait se poser pour tester sa cybersécurité?
PS: Tout d'abord, une entreprise ou une organisation doit se demander contre quels risques et quels acteurs elle souhaite se protéger. S'agit-il par exemple d'une protection contre la concurrence déloyale, un acteur étatique ou un hacker amateur? Ensuite, elle doit pouvoir identifier les risques qu'elle est prête à prendre. C'est probablement une bonne idée de réaliser un test d'intrusion tout en gardant à l'esprit qu'un test de x jours représentera ce qu'un pirate pourrait envisager après x jours de recherche. Cependant, il faut faire attention au fait que, pour que le test soit utile, il faut impérativement que le périmètre et le nombre de jours pris en compte soient représentatifs.

Comment s'informer au sujet des dernières nouvelles en la matière?
Béat Kunz: Des événements dédiés au thème de la cybersécurité contribuent largement à informer le public et les experts sur les principales cybermenaces qui nous guettent. Ensuite, il y a des associations professionnelles qui se focalisent sur la sécurité informatique. Enfin, les associations patronales et les médias participent activement à mettre en exergue les dangers auxquels nous devons faire face.

La formation, représente-t-elle une solution importante dans ce cadre?
BK: Bien entendu, c'est même essentiel! Les EPF, les Universités et les HES ont fait un travail considérable en mettant sur pied des filières de formation dédiées à la cybersécurité. La Confédération, le Département fédéral de la défense et notamment les Polices cantonales participent très activement à l'effort de formation consacré à ce thème. Melani joue un rôle d'information fondamental comme centrale d'enregistrement et d'analyse pour la sûreté de l'information.

Paul Such, CEO de Hacknowledge SA et Béat Kunz, CEO de Swiss Cyber Security Days (scsd.ch)

Et quelle est l'importance d'évènements et conférences traitant du thème de la cybersécurité?
BK: Ils sont essentiels car ils permettent l'échange d'informations et représentent donc une formidable plateforme de réseautage et de formation. Ces évènements et conférences sont d'ailleurs une vitrine des principaux prestataires en sécurité informatique.

Que retenir de la crise sanitaire de Covid-19 en termes de cybersécurité?
BK: Je pense que l'usage d'Internet, notamment pour le télétravail, fait que le public a pris davantage conscience du rôle joué par les technologies dans l'opérationnel des entreprises et dans les échanges interpersonnels. Dans ce cadre, les failles de sécurité sont perçues comme des défauts graves et inacceptables, moralement répréhensibles. Aujourd'hui, l'usager exige davantage d'éthique des développeurs pour protéger ses données.

Comment voyez-vous le futur en termes de cybersécurité?
BK: Les dépenses relatives à la protection des données liées aux infrastructures ou aux individus vont croître très sensiblement ces prochaines années. De même, les États investissent des moyens considérables pour la cyberdéfense et pour contrecarrer les attaques terroristes. Selon le WEF (forum économique mondial), les cyberattaques feront partie des dix risques les plus importants de notre planète dans les dix années à venir. Ce thème nous concerne donc tous, sans exception!

www.jbcsolutions.ch

Siège
Rue de la Vernie 12
1023 Crissier
T. +41 21 706 60 80

Agence
Route des Grives 2
1763 Granges-Paccot
T. +41 26 422 27 27