Akerva lance un centre de Cyberdéfense
DÉDIÉ ETI ET PME

Créé en 2013, et basé à Rennes, ce cabinet de conseil en cybersécurité et management des risques a le vent en poupe. Avec aujourd'hui 70 collaborateurs, des clients du CAC 40, une forte croissance et une prévision de chiffre d'affaires de 8 millions en 2020, Akerva entend redonner la confiance numérique indispensable à toutes les entreprises. Rencontre avec Laurent Delaporte, Président d'Akerva.

Les différentes offres « cybersécurité »

Quatre pôles d'expertise sont ainsi répertoriés, « nous avons des activités très techniques avec des audits, type tests d'intrusion, externes et internes. Nous prenons la place par exemple d'un collaborateur sans droits privilégiés particuliers ». Une équipe de quinze personnes à forte technicité intervient sur cette activité « nous développons les audits spécifiques appelés Red team, très demandés par les clients ».

Autre axe, la gouvernance, « nous accompagnons les clients sur l'aspect organisation, leurs politiques de sécurité du SI, les analyses de risques, les qualifications et certifications ISO27001 et ISO27005, nos clients ici sont principalement des entreprises dans le domaine Banque & Finance ».

Troisième activité, le monde l'IoT et des systèmes industriels. « Pour l'IoT en environnement de production, nous auditons des sites industriels à tout moment, ces clients français sont installés aux quatre coins du monde ». La mixité des audits techniques permet de détecter d'éventuelles failles remettant en cause la sécurité de l'usine et de s'assurer, sur le plan organisationnel, de la mise en place de bonnes pratiques et de politiques de risques autour de la cybersécurité. « Nous pouvons aussi intervenir sur la détection de failles sur une partie du système en environnement de conception ».

Enfin, le développement de modules e-learning « modules spécifiques destinés aux professionnels de l'IT, aux DBA, responsables infra systèmes réseaux, de quelques heures à plusieurs jours de formation, avec différents niveaux ». Cette approche est très qualifiante, « les grands comptes demandant de plus en plus que les prestataires aient une information très avancée sur les bonnes pratiques en termes de cybersécurité ».

« Les grands comptes demandant de plus en plus que les prestataires aient une information très avancée sur les bonnes pratiques en termes de cybersécurité ».

Laurent Delaporte

Un centre de cyberdéfense dédié ETI & PME !

« Si nous travaillons avec des entreprises du CAC 40, banques, assurances et industries, nous avons développé un centre de cyberdéfense destiné aux ETI, grosses PME et PME à risques ». Il s'agit d'un SOC où l'on va infogérer la sécurité de ces entreprises en proposant la mise en œuvre d'un environnement sécurisé et en inculquant des bonnes pratiques, mais aussi « s'assurer avec un système de remontées de l'ensemble des logs sur le dispositif sécuritaire, que l'entreprise ne soit pas victime d'attaques ou de vulnérabilités ».

Cette offre démarrée en janvier 2020 répond à un besoin croissant de cybersécurité des ETI et PME qui n'ont pas forcément les moyens financiers et structurels, « les équipes cybersécurité dédiées nécessitent beaucoup de professionnels dans une entreprise et souvent les équipes informatiques sont déjà bien réduites ! ».

« Nous proposons donc à ces entreprises un niveau de sécurité maximale à un coût moindre puisque nous utilisons l'ensemble de nos savoir-faire et de nos dispositifs ».

Défier la menace cyber en permanence !

Le risque intrinsèque de vols de données, de fraudes et d'arrêts de la production est réel, « les séquences financières lourdes ont des conséquences en termes d'images, de réputation ».

Aujourd'hui, les PME sont préoccupées par leur capacité ou incapacité à faire face à la menace cyber, « les patrons de PME ont conscience de la mesure du risque ».

« Les séquences financières lourdes ont des conséquences en termes d'images, de réputation ».

La mesure de l'exposition au risque est désormais un enjeu majeur pour l'entreprise et les tiers « il faut démontrer en permanence que l'entreprise n'est pas exposée ».

> Par Sabine Terrey