Auditer en continu son parc : un élément clé d'une gouvernance sécurité efficace

L'usage du numérique connait chaque année une croissance exponentielle au sein des entreprises de toutes tailles. Dans ce contexte, les parcs informatiques ne cessent de se développer et de nouveaux équipements sont déployés à la hâte pour leur permettre de rester compétitives et de mener à bien leurs opérations. Si le digital est une formidable opportunité de gagner en productivité et en agilité, il est également une source de danger faute d'être encadré et maitrisé. Chaque mois ce sont en effet plus de mille failles de sécurité qui sont ainsi découvertes, avec à la clef une explosion du nombre de cyberattaques. Alors, comment faire pour mesurer son exposition au risque, la réduire et évoluer dans une sphère de confiance pour pouvoir se développer sereinement ?

Bien connaitre ses assets

La première chose à prendre en considération est de connaitre précisément ses actifs et son parc. Cette cartographie précise permettra de s'assurer que tous les équipements connectés au système d'information sont identifiés. Cette tâche est permanente et doit couvrir tous les types d'équipement, ordinateurs, devices, mobiles, logiciels, serveurs, etc., sans oublier les objets connectés de toutes sortes qui connaissent aujourd'hui une forte croissance y compris dans le secteur professionnel.

Prendre en compte la notion d'approche récurrente

Dans ce contexte, le sujet de l'audit continu prend tout son sens et semble devenir un incontournable de la gouvernance cybersécurité des entreprises. En effet, imposée par la réglementation à certains secteurs et entreprises stratégiques (OIV, etc.), la gestion des vulnérabilités occupe désormais une place grandissante auprès des PME et ETI. Ces dernières cherchent à se conformer aux recommandations de l'ANSSI car elles savent qu'elles sont aujourd'hui les plus impactées par les cyberattaques. Grâce à l'analyse continue, elles sont alors en mesure d'avoir une vue temps réel de leur parc informatique, de mesurer leur exposition au risque en identifiant les vulnérabilités. Elles ont alors les capacités d'agir préventivement ou de réagir pour accroitre la sécurité du système d'information. Les entreprises ne restent donc pas passives et peuvent réellement piloter leur gouvernance cyber de manière dynamique et permanente.

Les solutions sur le marché sont nombreuses…mais ne se valent pas toutes

Si les solutions d'inventaires de parc informatique sont légion, les solutions de mesure en continu des vulnérabilités sont moins nombreuses. Elles ont chacune leur spécificité et pour faire le bon choix il convient donc de se poser les bonnes questions :
– Le déploiement de la solution nécessite-t-il des compétences spécifiques (en particulier s'il faut l'installer sur des petits sites distants) ?
– La solution va-t-elle impacter le réseau et indirectement la production informatique ?
– Quel est le niveau de détail fourni et est-il compréhensible uniquement par des experts ?
– A quelle fréquence la solution est-elle mise à jour quand on sait que des nouvelles failles sont

publiées quotidiennement ?
– Les informations sensibles de l'entreprise seront-elles collectées et stockées dans le cloud ?

Un levier pour progresser à tous les niveaux

Au-delà de la mesure des vulnérabilités ce sont les actions de remédiation dans la durée qui permettront à l'entreprise de mieux se protéger. C'est pourquoi les solutions d'audit les plus avancées proposent à la fois des système de notation simple à comprendre (pour un pilotage macro au niveau Direction) mais également des recommandations fines en matière de correction (pour une mise en action par les équipes opérationnelles). Le DSI d'un équipementier automobile avait ainsi pour habitude de publier tous les mois l'évolution de son « indice cyber ». Il en avait fait un moteur de motivation pour son équipe afin qu'elle le fasse progresser et un levier de sensibilisation à la cybersécurité pour les autres Directions.

L'audit continu est donc une opportunité pour tous de poser les bases d'une gouvernance cybersécurité moderne et efficace. Indispensable, il permettra de faire des choix éclairés, de connaitre ses assets et de travailler dans un cadre sécurisant.

Thierry Balian
Directeur Business Unit Cybersécurité – Foliateam