Ecrit par Echo du Mardi le 19 janvier 2022

Cybersécurité et postes de travail : vers une stricte limitation aux usages professionnels ?

À quelques exceptions près, en particulier dans les secteurs les plus sensibles, l'habitude est souvent prise d'utiliser son poste de travail professionnel pour certains (si ce n'est tous) usages personnels. D'autant plus lorsqu'il s'agit d'un poste portable. Or, ce sont ces postes qui constituent le vecteur le plus 'efficace' des malveillances à l'encontre du SI (Système d'information) des organisations. Dès lors, peut-on imaginer un monde aux usages numériques professionnels et personnels strictement étanches ?

Postes de travail : une porte ouverte vers l'ensemble du SI

Par principe, les attaques malveillantes à l'encontre des entreprises ou administrations ont généralement deux objectifs, bien souvent couplés : l'argent et l'information. Et dans tous les cas, elles sont menées via des méthodes industrielles, assurant efficacité et reproductibilité aux assaillants.

Ecrit par Echo du Mardi le 19 janvier 2022

Parmi ces méthodes, le piratage de réseaux Wifi non protégés est efficace, mais il nécessite un accès physique. Les attaques de serveurs mal protégés peuvent créer des dégâts, mais ils restent souvent circonscrits à leurs environnements applicatifs. Il est aussi possible de s'attaquer au VPN-SSL de l'organisation lorsque celui-ci est vulnérable. Mais rien n'est comparable à la réussite du ciblage utilisateurs, par mail (phishing) ou surf (implantation de logiciels malveillants sur les postes via des sites web corrompus).
Même bien protégé, le poste utilisateur reste de loin le plus vulnérable car, par définition, il est connecté à 'l'Active directory' de l'entreprise (l'outil d'annuaire le plus représenté sur le marché). Et cette solution, malgré l'effort des développeurs, reste sujette à de nombreuses vulnérabilités permettant l'accès distant et l'élévation de privilèges depuis un compte utilisateur. C'est la porte ouverte au fameux « admin access » et à l'ensemble des données de l'entreprise.

Une cybersécurité proactive et transparente pour l'usager
Pour se prémunir au maximum de ces risques, rien de plus simple a priori : en plus des logiciels de cybersécurité dédiés, il suffirait de maintenir ses postes de travail à jour, pour éviter l'exploitation de failles connues. Certes, mais c'est encore sans compter sur les failles Zero Day, sur lesquelles les cyberattaquants sont de plus en plus productifs.
Pour contrer ces risques, la mise en œuvre de solutions capables de bloquer des actions non habituelles des applications ou du système demeure une pratique efficace, car proactive. Par essence en effet, les logiciels malveillants ont des comportements très spécifiques, cherchant tout type d'ouverture pour s'introduire et modifier les systèmes.
Dans tous les cas en revanche, ces outils doivent être le plus transparent possible pour l'usager, afin qu'il puisse accomplir sereinement ses tâches quotidiennes et ne pas perdre en productivité du fait de blocages permanents. Ce qui ne doit en rien l'empêcher de rester vigilant pour autant.

Sébastien Viou.

Pour toujours en savoir plus, lisez **www.echodumardi.com**, le seul média économique 100% Vaucluse habilité à publier les annonces légales, les appels d'offres et les ventes aux enchères !

Ecrit par Echo du Mardi le 19 janvier 2022

Au-delà des chartes d'utilisation, vers un usage strictement professionnel des postes de travail ?

En dehors de quelques secteurs manipulant des données sensibles où les postes de travail sont très verrouillés et limitent au strict minimum les usages, nombreux sont les utilisateurs à se servir de leur poste de travail pour leurs usages personnels. Allant souvent même jusqu'à autoriser leurs enfants à s'en servir, ou jouer en réseau avec. Une situation sans doute encore exacerbée avec l'accélération du télétravail, quand ce n'est pas l'entreprise qui demande au collaborateur d'utiliser sa machine personnelle pour ne pas avoir à payer une machine professionnelle.

Si un certain nombre d'organisations ont mis en place des chartes d'usages et des outillages informatiques mis à disposition de leurs collaborateurs, dans les faits, peu d'entre elles appliquent des sanctions en cas de comportements imprudents, même s'il en résulte des situations particulièrement graves pour l'ensemble du système d'information (perte, vol de données ou ransomwares, etc.).

Avec le développement de l'informatique domestique (smartphones, tablettes, PC, accès internet), associé à des risques numériques toujours plus importants pour les organisations, peut-être est-il temps pour ces dernières de limiter strictement aux usages professionnels les outils numériques de l'entreprise mis à disposition de leurs collaborateurs.

Dans ce cas, on parlerait d'outils numériques de service (uniquement à usage professionnel) et non plus d'outils numériques de fonction (à usage « global » du salarié). Cela ne résoudra pas tous les problèmes en matière de cybersécurité, mais pourrait a minima contribuer à cyber-responsabiliser les collaborateurs et ainsi à l'amélioration des usages.

Tribune de Sébastien Viou, directeur cybersécurité produit et 'cyber-évangéliste' chez Stormshield, spécialiste et éditeur français de logiciels spécialisés en sécurité informatique

Pour toujours en savoir plus, lisez **www.echodumardi.com**, le seul média économique 100% Vaucluse habilité à publier les annonces légales, les appels d'offres et les ventes aux enchères !