SOLUTIONS MANUTENTION
LE MAGAZINE DES ÉQUIPEMENTS ET SOLUTIONS EN ENTREPÔTS

L’avis du PRO

5 conseils de sécurité pour bien protéger ses postes de travail

La sécurité des postes de travail ressemble à un serpent de mer. Avec une économie toujours plus dépendante du numérique et des postes de travail toujours plus mobiles, la moindre vulnérabilité exploitée peut devenir catastrophique. Pour autant, les méthodes et solutions de sécurisation s’adaptent à ces nouvelles contraintes

Découvrir la primo-infection le plus tôt possible

S’emparer des données personnelles, industrielles ou commerciales sensibles, pour les chiffrer et les rançonner, les publier ou encore perturber la production de l’entreprise, constitue l’objectif principal des attaquants. Dans ce but, ils doivent trouver des “portes d’entrée” qui sont bien souvent des machines utilisateurs. Ces dernières, une fois compromises, et même sans privilèges élevés, leur permettent alors de pénétrer le système plus en profondeur. Pour y parvenir, les attaquants peuvent à la fois exploiter des failles humaines, avec du phishing de plus en plus ciblé (spear phishing) ou des failles de systèmes mal protégés : serveurs RDP exposés sur Internet, applications non mises à jour, etc. Avant que ces attaquants ne puissent aller plus loin dans le système, il s’agit d’identifier ces attaques dès qu’elles surviennent, afin d’arrêter le processus malveillant, et bloquer immédiatement leur propagation sur la machine ou l’application concernée.

Adapter le niveau de sécurité au contexte environnemental

Assurer la sécurité des postes de travail n’était déjà pas simple dans l’enceinte même de l’entreprise. Avec la multiplication des PC portables et surtout les enjeux de mobilité propres à chaque organisation, la mission s’est encore complexifiée. Dès

lors, le niveau de protection des postes de travail ne peut plus se contenter d'être statique, mais doit devenir dynamique, en fonction du contexte et des différents scenarii de mobilité au sein de l'organisation. Il s'agit par exemple de maîtriser les réseaux WiFi autorisés, de les désactiver lorsqu'une connexion LAN est disponible ou encore d'empêcher toute autre connexion que le VPN lorsque celui-ci est actif (pour éviter les attaques par rebond).

Focaliser la protection sur l'agent dans une approche comportementale

Il est toujours plus simple et moins risqué d'identifier un élément malveillant dès l'entrée (poste de travail ou serveur), avant qu'il n'ait pu se propager, et afin de bloquer immédiatement ses activités. C'est tout l'objectif des systèmes de protection des postes de travail. Pour contrer les ransomwares qui deviennent de plus en plus en sophistiqués, les antivirus traditionnels, qui s'appuient sur des signatures, ne sont pas suffisants. Les attaques inconnues de type ZeroDay ne peuvent tout simplement pas être immédiatement détectées. Pour pallier cette déficience, le HIPS comportemental fonde ses analyses sur le comportement "normal" d'un hôte ou de ses applications. En cas d'activité suspecte des applications légitimes, le système remonte immédiatement une alerte (ou bloque immédiatement les activités) afin de limiter les risques de propagation. Un peu plus complexe à mettre en œuvre, il s'adapte en revanche facilement à tout type d'organisation et sera en mesure de contrer des attaques inconnues de type ZeroDay.

Bloquer proactivement les attaques et prévoir les attaques futures

Savoir interrompre une attaque, connue ou non, est bien sûr essentiel. Mais pour aller plus loin, il s'agit aussi d'apprendre de ces attaques, afin de les prévenir encore plus facilement à l'avenir. C'est l'un des rôles qu'il est possible d'attribuer aux solutions Endpoint Detection & Response (EDR) : outre la réponse immédiate, l'examen de leurs logs permet, après une analyse approfondie, d'optimiser l'efficacité des solutions dans la recherche d'attaques. Deux approches sont possibles dans ce contexte. L'approche focalisée sur une solution Cloud s'appuie sur la remontée d'un agent léger déployé sur chaque poste et apporte toute la promesse de l'intelligence artificielle avec, néanmoins, l'obligation de postes connectés. À l'opposé, une solution basée sur un agent autonome assure la protection proactive temps réel de chaque poste, tout en fournissant les informations pour une analyse ultérieure de l'attaque. Des systèmes tiers pourront alors intégrer ces évènements pour les corréler dans un contexte d'intelligence artificielle.

S'assurer de la sécurité du système de protection lui-même

Les données des organisations sont l'objectif principal des cyber-attaquants. Mais les systèmes de sécurité des organisations demeurent des cibles primaires privilégiées. En effet, si les attaquants parviennent à désactiver les protections, ou pire, à utiliser les droits des comptes à privilèges de ces solutions, la porte du système d'information leur est alors grande ouverte. Au même titre que le déploiement de n'importe quel matériel ou application, il s'agit de limiter au maximum les risques de bug ou d'apparition de vulnérabilité, en appliquant par défaut une configuration durcie et adéquate, compte tenu de la surface d'attaque qu'ils représentent. Avec des droits privilégiés, celle des systèmes de protection demeure relativement vaste. Une approche Security by Design dans leur développement est donc à favoriser. ● Mark Johnson, ingénieur avant-vente Stormshield Endpoint Security. Les technologies

Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l’IT et de l’OT afin de protéger les activités de ses clients.