Cybersécurité pour Microsoft 365 – il en faut plus

Microsoft 365 gagne en popularité. Certes, les fonctions de sécurité intégrées se sont améliorées au cours des dernières années, mais elles présentent encore des lacunes. Des solutions de fournisseurs tiers apportent souvent le plus de sécurité nécessaire. Patrick Michel, Principal Consultant chez le distributeur de sécurité informatique BOLL, nous en dit plus.

Microsoft 365 contient également des fonctions de sécurité. Celles-ci protègent-elles de manière fiable contre les cybermenaces actuelles?
Microsoft a fortement amélioré la protection contre les menaces au cours des dernières années et offre une bonne défense contre les logiciels malveillants connus. Pour les menaces de plus en plus sophistiquées et encore inconnues, comme les advanced persistent threats (APT) et les ransomwares, les solutions des fabricants spécialisés sont toutefois nettement plus avancées. Et ce, surtout en ce qui concerne la sécurité des e-mails et des endpoints ainsi que l'analyse du stockage en ligne, comme par exemple dans OneDrive, Teams et SharePoint.

En quoi les fabricants spécialisés se distinguent-ils?
Ils se concentrent entièrement sur la sécurité, ont une longue expérience et un vaste savoir-faire. En même temps, ils font preuve d'innovation et développent de nouvelles technologies, parfois disruptives, qui élèvent la cybersécurité à un niveau supérieur. Si ces spécialistes ne faisaient pas du bon travail et n'avaient pas d'atouts à faire valoir par rapport à des fournisseurs actifs à grande échelle comme Microsoft, ils pourraient ne plus exister du tout. Un autre aspect ne doit pas être oublié: l'homme et son comportement sont toujours au centre de la sécurité – et les formations de sensibilisation à la sécurité, telles qu'elles sont proposées par diverses entreprises spécialisées, peuvent largement contribuer à l'améliorer.

L'expert en sécurité informatique Patrick Michel est Principal Consultant chez le distributeur de sécurité informatique BOLL.

Quels sont les fournisseurs qui offrent une meilleure protection des terminaux?
Les terminaux avec lesquels on accède à Microsoft 365 se trouvent partout – du bureau de l'entreprise au bureau à domicile en passant par la place d'un café. Une protection des terminaux hautement efficace est donc extrêmement importante. Des fournisseurs comme Palo Alto Networks, Rapid7, Kaspersky et WatchGuard utilisent de plus en plus le machine learning pour renforcer et automatiser la défense contre les codes malveillants inconnus. L'entreprise Deep Instinct suit une approche très intéressante.

Quelle est la particularité de la solution de Deep Instinct?
Deep Instinct mise sur la prévention plutôt que sur la réaction «after the fact» et utilise pour cela le deep learning. Il s'agit d'une variante avancée du machine learning qui se passe de «formateurs» humains. Deep Instinct a développé à cet effet le seul cadre

d'apprentissage profond adapté à la cybersécurité. Le réseau neural apprend automatiquement à partir de millions de fichiers et de scripts, bons ou malveillants, et reconnaît ainsi l'«ADN» des menaces. Deep Instinct fait entièrement confiance au deep learning et promet de repousser 99 % de tous les logiciels malveillants inconnus..

En quoi cela contribue-t-il à la protection des terminaux?
Sur la base des connaissances du réseau neural, on obtient ce que l'on appelle le cerveau Deep Instinct. Celui-ci constitue le noyau de l'agent léger qui est installé sur les endpoints, n'utilise que peu de ressources système et ne doit être actualisé qu'une à deux fois par an. L'agent détecte et stoppe les menaces telles que les ransomwares en moins de 20 millisecondes, ce qui les empêche de déployer leurs effets néfastes. De plus, il n'a pas besoin d'une connexion Internet permanente – un atout idéal même dans des environnements OT et de haute sécurité cloisonnés.

Venons-en à la sécurité des e-mails: quelles solutions contribuent à l'améliorer?
Ici aussi, les spécialistes ont plus à offrir. Proofpoint en est un exemple avec ses solutions pour les grandes entreprises et les PME. Il propose notamment la protection contre les menaces avancées (targeted attack protection) pour lutter contre les menaces ciblées et complexes avant qu'elles n'atteignent la boîte aux lettres d'un collaborateur. Elle inclut le sandboxing, une technologie permettant de vérifier de manière isolée les codes malveillants potentiels – une caractéristique pour laquelle Microsoft, même dans sa variante ATP, n'obtient souvent pas de bons résultats lors des tests. Une boîte de réception de secours permet en outre de continuer à travailler avec les e-mails si Microsoft 365 devait tomber en panne.

Le cryptage des e-mails est un sujet trop compliqué pour beaucoup. Existe-t-il une solution?
La solution du fournisseur suisse SEPPmail simplifie considérablement le cryptage et la signature des e-mails grâce à la gestion automatisée des certificats au niveau de la passerelle et à d'autres fonctions comme le cryptage de domaine. Ainsi, les certificats numériques ne doivent pas être commandés individuellement pour chaque utilisateur et installés dans Outlook. Le cryptage et la signature se font de manière totalement transparente. Cette solution haut de gamme est disponible sous forme d'appliance et, depuis peu, également dans le cloud.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15,
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch
www.boll.ch

→ **www.boll.ch**