Sécurité maximale pour Microsoft 365

Toute personne utilisant Microsoft 365 doit prêter une attention particulière aux aspects de sécurité. L'utilisation de solutions de sécurité complémentaires est souvent recommandée. Patrick Michel, consultant principal chez le distributeur de sécurité informatique BOLL, explique les aspects importants de la sécurité dans une interview.

Microsoft 365 et la sécurité – comment cela s'accorde-t-il?
Tout d'abord, il faut souligner que Microsoft est clairement le leader du marché en termes de groupware, c'est-à-dire Exchange avec le courrier électronique et le calendrier. De plus en plus d'entreprises ne s'appuient plus sur leur propre serveur Exchange, mais sur Microsoft 365, dont l'ensemble des fonctionnalités et de la sécurité sont externalisées dans le cloud. Il est également important de préciser que la communication par courrier électronique reste le principal vecteur utilisé lors des cyberattaques et que le courrier électronique est utilisé intensivement dans presque toutes les organisations. La sécurité joue donc un rôle extrêmement important dans le cadre de Microsoft 365.

Microsoft 365 offre diverses fonctions de sécurité intégrées. Ces «outils embarqués» sont-ils suffisants?
Lorsqu'il s'agit de logiciels malveillants connus, Microsoft 365 offre de bonnes performances de détection et de défense. Cependant, pour les menaces encore inconnues, les APT (Advanced Persistent Threats) et ransomwares – dont les méthodes d'attaque utilisées par les cybercriminels sont de plus en plus sophistiquées – les solutions spécialisées de sécurité du courrier électronique de fabricants tels que Proofpoint, Kaspersky et Fortinet sont plus efficaces. Par exemple, la détection de logiciels malveillants connus et inconnus se fait de préférence via le sandboxing. Microsoft 365 ne propose cette option que dans le pack Premium et selon des tests indépendants, il existe de meilleures solutions de sandboxing sur le marché.

Le stockage évolue également de plus en plus vers le cloud. Que devez-vous considérer ici?
Il ne s'agit pas seulement d'espace de stockage en soi – comme OneDrive: les entreprises se tournent de plus en plus vers différentes applications SaaS qui contiennent leurs propres pools de données autonomes. Les données sont alors stockées sur différentes plateformes et il devient difficile d'en garder une vue d'ensemble et de s'assurer que seules les personnes autorisées peuvent y accéder.

Qu'est-ce qui peut aider dans ces environnements multi-cloud ou multi-SaaS?
C'est là qu'interviennent les Cloud Access Security Brokers (CASB). Ils forment une solution centrale et automatisée pour contrôler l'accès à tous les services cloud utilisés. Le CASB deviendra aussi important à l'avenir que les pare-feux le sont aujourd'hui. Le service CASB lui-même est également souvent proposé en tant que service SaaS. Le contrôle des utilisateurs autorisés à accéder aux services et aux données sera donc à nouveau centralisé. Cependant, les fonctions sont multiples. Par exemple, un CASB peut également détecter lorsqu'un utilisateur se connecte brièvement depuis des endroits complètement différents, puis déclencher l'alarme. Microsoft a également une solution dans ce domaine avec Cloud App Security, mais elle est principalement conçue pour une intégration étroite avec les propres applications et services de l'entreprise. Les produits CASB de fabricants spécialisés tels que Bitglass sont plus universels et offrent des fonctions supplémentaires.

Qu'en est-il de la protection classique des endpoints?
Les terminaux utilisés pour accéder à Microsoft 365 se trouvent aujourd'hui partout: au siège de l'entreprise, au bureau à domicile, en déplacement dans le train, dans un café ou un espace de coworking – en d'autres termes, en dehors du réseau de l'entreprise. La protection des terminaux est donc d'une grande importance. La solution de protection utilisée ne doit pas se limiter à la détection basée sur la signature de logiciels malveillants connus, les solutions de sécurité des terminaux doivent plutôt être capables de détecter et éliminer les logiciels malveillants et les méthodes d'attaque les plus avancées jusqu'alors inconnus, avant qu'ils ne puissent compromettre l'entreprise. C'est un domaine où l'intelligence artificielle est de plus en plus utilisée, comme dans «Traps» de Palo Alto Networks.

L'expert en sécurité informatique Patrick Michel est consultant principal chez le distributeur de sécurité informatique BOLL.

Malgré toute la technologie: on dit aussi que le point faible le plus important est l'être humain ...
C'est vrai, et c'est exactement pourquoi il est essentiel, surtout à l'ère du cloud, de sensibiliser tous les employés aux aspects de la sécurité par le biais de formations – obligatoires, continues et vérifiables. Avec une formation continue en matière de sécurité, vous gagnez grandement en sécurité. À cette fin, il existe diverses plateformes de formation pour la sensibilisation à la sécurité – comme celles de Kaspersky et Proofpoint – qui conviennent également aux PME. Ces solutions automatisent la formation, vérifient entre autres la réaction des employés face aux courriels de phishing et répètent tout ce qui n'a pas été résolu correctement jusqu'à ce que ce soit intégré. Ainsi, une formation individuelle à la cybersécurité est possible sans presque aucun effort supplémentaire.

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