Kaspersky Security Awareness: Plus de sécurité grâce à la sensibilisation des employés

Au cours des dernières années, le nombre d'attaques de phishing et de logiciels malveillants est monté en flèche. Ces attaques sont de plus en plus souvent dirigées contre les employés, car ceux-ci représentent souvent l'une des plus grandes lacunes dans la sécurité dans l'entreprise. La sensibilisation à la sécurité peut changer cela par la formation et le renforcement des compétences.

La sécurité informatique n'est plus un sujet de niche. En raison de l'augmentation de l'espionnage et des piratages, la sécurité informatique est devenue ces dernières années un sujet problématique et déterminant qui ne concerne plus seulement les spécialistes de la sécurité. Le nombre d'appareils connectés au réseau est en constante augmentation et les données deviennent de plus en plus importantes et précieuses. Par conséquent, les attaquants obtiennent généralement un accès immédiat à toutes les informations de l'entreprise et aux données personnelles. En outre, les entreprises sont confrontées à des scénarios de menace de plus en plus variés car la cybercriminalité prend des dimensions totalement nouvelles et se professionnalise continuellement.

En plus des pertes financières, il y a aussi la menace d'atteinte à la réputation

Les bandes criminelles à motivation financière représentent l'un des plus grands risques pour la sécurité. Ils sont très motivés, extrêmement professionnels, très bien équipés et bien formés. Bien que la plupart des entreprises soient conscientes des dangers posés par le crime organisé, l'étude de Kaspersky «Digital Culture At Work» montre que les employés ne sont que peu ou pas suffisamment formés en matière de sécurité informatique. En outre, 60% des appareils des employés contiennent des informations confidentielles telles que des données financières ou des bases de données de messagerie électronique et 80% des employés ne se sentent pas responsables de la protection de leurs données. Les attaquants profitent de cette ignorance et du manque de sensibilisation à la sécurité informatique. Les criminels sur Internet ont de plus en plus recours à des méthodes d'ingénierie sociale, de Spear-Phishing, de crypto-extorsion et de fraude des CEO. L'ouverture irréfléchie d'un e-mail inconnu suffit à compromettre toute la sécurité. En quelques minutes, le malware infecte l'ensemble du réseau de l'entreprise. Environ 80% des incidents de

sécurité informatique peuvent être attribués à une conduite inconsciente des employés. Cela se traduit par des pertes financières s'élevant à des milliards d'euros dans le monde entier. Les entreprises doivent craindre non seulement des pertes financières après des failles de sécurité, mais aussi une atteinte à la réputation. Cependant, le personnel peut facilement être exclu comme facteur de risque par une formation compétente et efficace. C'est précisément là qu'interviennent la solution Security Awareness.

Security Awareness met l'accent sur un changement de culture durable

Les formations en sécurité informatique n'ont un véritable sens que si elles ont des effets à long terme. L'objectif devrait toujours être un changement de culture dans l'entreprise, car c'est la seule façon de promouvoir la sécurité de l'entreprise à long terme. Les entreprises spécialisées dans la sécurité informatique, comme Kaspersky, fournisseur du distributeur de sécurité informatique Boll Engineering SA, proposent des formations pour sensibiliser les collaborateurs à la sécurité avec leurs programmes en ligne. Ces plateformes peuvent être mises en place rapidement et sont faciles à gérer. Elles offrent aux utilisateurs la possibilité de fixer leur propre rythme d'apprentissage et de répéter les modules individuels selon les besoins. L'éventail des sujets est diversifié: de la sécurité du courrier électronique et du phishing à la protection des données et à l'utilisation sûre des appareils mobiles. La méthodologie des cours de formation est spécialement conçue pour s'adapter aux caractéristiques de la mémoire humaine. Ainsi, le contenu de l'apprentissage est enseigné de manière multimodale, par exemple par des attaques de phishing simulées et par intervalles. Il est ainsi plus facile pour le participant de mémoriser à long terme les connaissances nouvellement acquises. Les résultats montrent que la sensibilisation des utilisateurs diminue les incidents de sécurité jusqu'à 90% et réduit les pertes financières de 50%. La formation professionnelle des employés en matière de sécurité est donc un facteur extrêmement important de la sécurité informatique des entreprises et ne doit pas être négligée.

Vous trouverez ici de plus amples informations sur le programme de formation en ligne Automated Security Awareness Platform (ASAP) de Kaspersky, fournisseur de Boll Engineering SA: **https://www.boll.ch/kaspersky/asap.html**

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