Alerte, cyberattaque

Numérisation Il n'est pas possible de se protéger à 100% contre les cybercriminels. Mais qui adopte le bon comportement en cas d'urgence possède un avantage décisif. Quels sont les réflexes à avoir juste après une attaque et comment s'y préparer en amont? Les conseils de notre expert.

Lucas Schult

Dans l'une de mes dernières chroniques, j'ai écrit qu'il n'y avait pas de honte à se faire piéger par une cyberattaque professionnelle. Oui, la plupart d'entre nous savent depuis longtemps qu'il faut se méfier des e-mails suspects et ne pas cliquer sur n'importe quel lien. C'est pourquoi nous pensons – et je n'y fais pas exception – que nous avons peu de chance d'être un jour concernés. Car nous sommes au courant et faisons preuve de prudence. Pourtant, les cyberattaques aboutissent régulièrement. Pourquoi? Parce que connaître les méthodes des cybercriminels ne suffit pas pour bien se protéger. La situation dans laquelle se trouve une personne joue notamment un rôle important. Le stress, les émotions, l'inattention, tout le monde peut être victime d'une cyberattaque: l'assistante médicale en formation comme la propriétaire du cabinet jusqu'aux professionnels de l'informatique qui travaillent tous les jours sur les questions de sécurité informatique. Malheureusement, même les meilleures mesures de protection n'offrent pas une sécurité à 100%. Et après une cyberattaque aboutie, le bon comportement joue un rôle important et détermine si celle-ci aura des répercussions graves ou non. C'est pourquoi je souhaiterais aujourd'hui vous donner quelques conseils sur la manière de vous comporter en cas d'urgence.

La parole est d'or

La première règle: se taire n'est définitivement pas une bonne option. Vous n'êtes pas entièrement sûr(e) de ne pas avoir cliqué sur un lien dangereux? Mieux vaut en avertir votre support ou partenaire informatique. Cela ne vaut pas seulement pour vous, mais pour toute votre équipe. Il est donc important que tous les membres de l'équipe sachent qu'ils ne seront pas sanctionnés si un tel incident devait se produire. C'est la seule façon de s'assurer que tout le monde agisse immédiatement – au lieu d'espérer que personne ne remarque sa propre inattention.

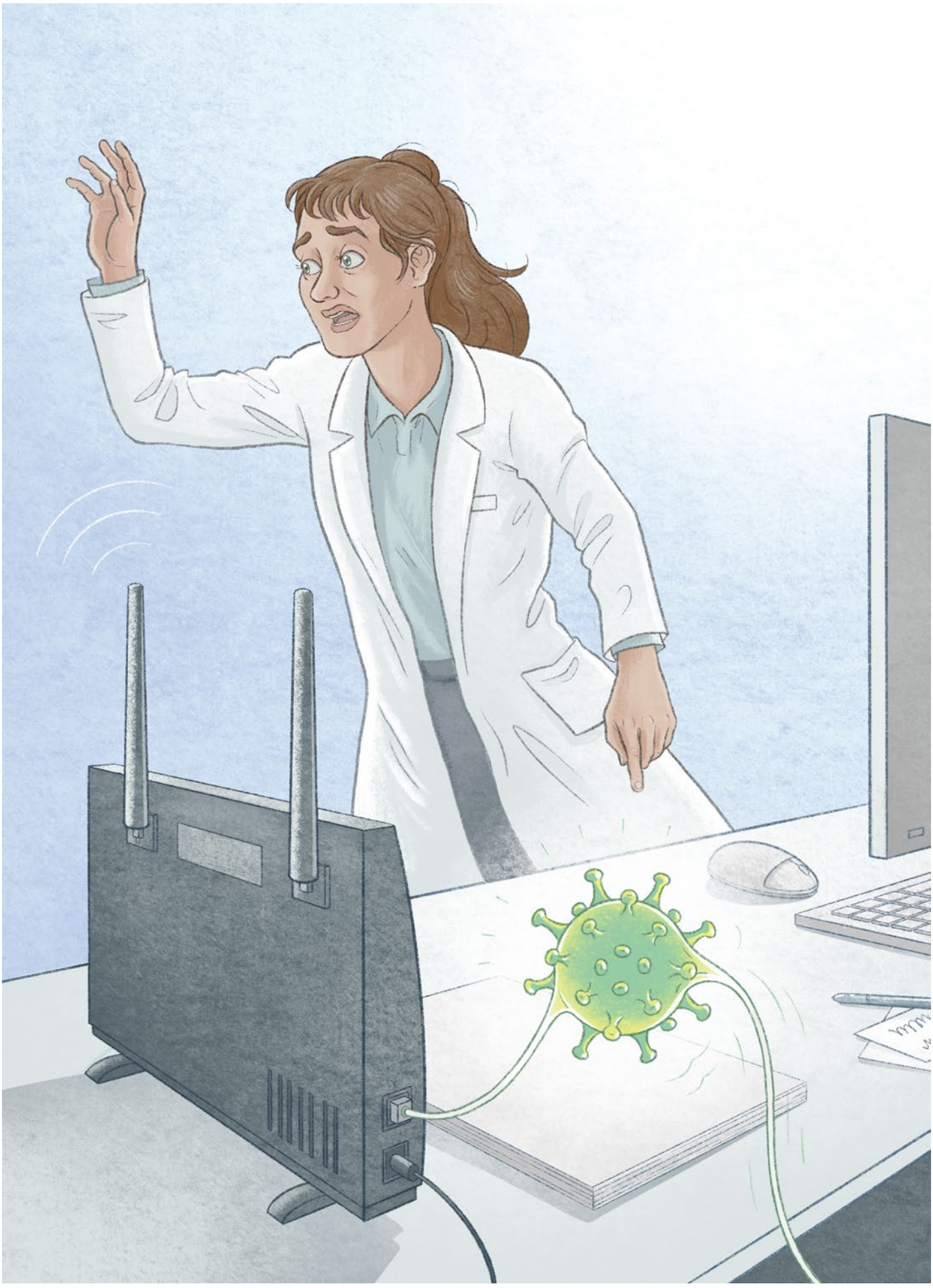
Mais que doit-on faire lorsqu'on est victime d'une cyberattaque? Le plus sûr est d'éteindre tous les systèmes: ordinateurs, portables, etc. Ensuite, éteignez également le routeur Wi-Fi et déconnectez le système du réseau. Vous pouvez ainsi éviter qu'un éventuel logiciel malveillant n'infecte d'autres systèmes. Faites ensuite immédiatement appel à votre support informatique afin qu'il puisse vous aider pour la suite. Il est important de décrire le plus précisément possible ce qui s'est passé: avez-vous ouvert un e-mail? Avez-vous cliqué sur un lien? Que s'est-il passé ensuite?

Vous devriez également informer tous les collaborateurs de votre cabinet, car vous n'êtes peut-être pas le seul ou la seule à avoir reçu un e-mail infecté... Votre support informatique peut alors, en prenant les précautions nécessaires (par exemple en désactivant le réseau), contrôler les autres ordinateurs et comptes de messagerie de votre cabinet et supprimer les messages malveillants de toutes les boîtes de réception et des corbeilles électroniques.

La bonne stratégie de sauvegarde

Et pour finir, je souhaiterais délivrer un dernier message qui me tient à cœur: bien préparer son cabinet en amont d'une éventuelle cyberattaque offre des avantages décisifs en cas d'urgence. Lors d'une attaque par un rançongiciel – ou ransomware – par exemple, une partie ou l'ensemble des données de votre cabinet sont cryptées par le pirate. Ce dernier réclame ensuite des sommes colossales pour vous donner le code de déchiffrement... Si vous avez investi en amont dans une stratégie de sauvegarde efficace en prenant en compte les attaques de rançongiciels, une éventuelle perte de données aura un impact seulement marginal. Si, en outre, vous complétez la stratégie de sauvegarde par une bonne sécurité des points d'accès (EPS), en mesure de faire face aux rançongiciels, vous mettez tous les atouts de votre côté. Une bonne préparation combinée à un comportement adéquat en cas d'urgence ne vous laisse donc pas, vous et votre cabinet, sans défense face aux cybercriminels.

Lucas Schult
est directeur (CEO) de HIN. Il écrit régulièrement dans cette rubrique à propos de la sécurité numérique.



© Luca Bartulović