Es kann uns alle treffen

Digitalisierung Einen 100-prozentigen Schutz vor Cyberkriminellen gibt es nicht. Wer sich aber im Ernstfall richtig verhält, hat einen entscheidenden Vorteil. Was Sie nach einer Attacke sofort tun sollten – und wie Sie sich bereits jetzt vorbereiten können.

Lucas Schult

In einer meiner letzten Kolumnen habe ich geschrieben, dass es keine Schande ist, auf eine professionelle Cyberattacke hereinzufallen. Ja, die meisten von uns wissen längst, dass man bei verdächtigen E-Mails vorsichtig sein und Links nicht wahllos anklicken soll. Deshalb denken wir – und mich selber schliesse ich hier nicht aus – dass es uns wohl kaum treffen wird. Denn wir wissen ja Bescheid und sind vorsichtig. Trotzdem sind Cyberattacken immer wieder erfolgreich. Warum? Weil das Wissen über die Angriffsmethoden Cyberkrimineller alleine keinen ausreichenden Schutz bietet. So spielt beispielsweise die Situation, in der sich jemand gerade befindet, eine wichtige Rolle. Stress, Emotionen, Unaufmerksamkeit – jede und jeder kann auf eine Cyberattacke hereinfallen, die lernende MPA ebenso wie die Praxisinhaberin – und auch IT-Profis, die sich tagtäglich mit IT-Sicherheit auseinandersetzen, sind nicht gefeit. Leider bieten selbst die besten Schutzmassnahmen keine 100-prozentige Sicherheit. Und nach einer erfolgreichen Cyberattacke spielt das richtige Verhalten eine wichtige Rolle und entscheidet darüber, ob diese schwerwiegende Folgen hat oder eben nicht. Deshalb möchte ich Ihnen heute Tipps geben, wie Sie sich im Ernstfall richtig verhalten.

Reden ist Gold

Zunächst einmal gilt: Schweigen ist definitiv keine gute Option. Sind Sie sich nicht sicher, ob Sie vielleicht gerade einen gefährlichen Link angeklickt haben? Dann fragen Sie lieber einmal zu viel als einmal zu wenig bei Ihrem IT-Partner oder IT-Support nach. Dies gilt nicht nur für Sie, sondern für Ihr gesamtes Team. Deshalb ist es wichtig, dass alle Team-Mitglieder wissen, dass ihnen keine Sanktionen drohen, sollte es einmal zu einem solchen Zwischenfall kommen. Nur so können Sie sicherstellen, dass jede und jeder sofort handelt – statt zu hoffen, dass niemand die eigene Unachtsamkeit bemerkt.

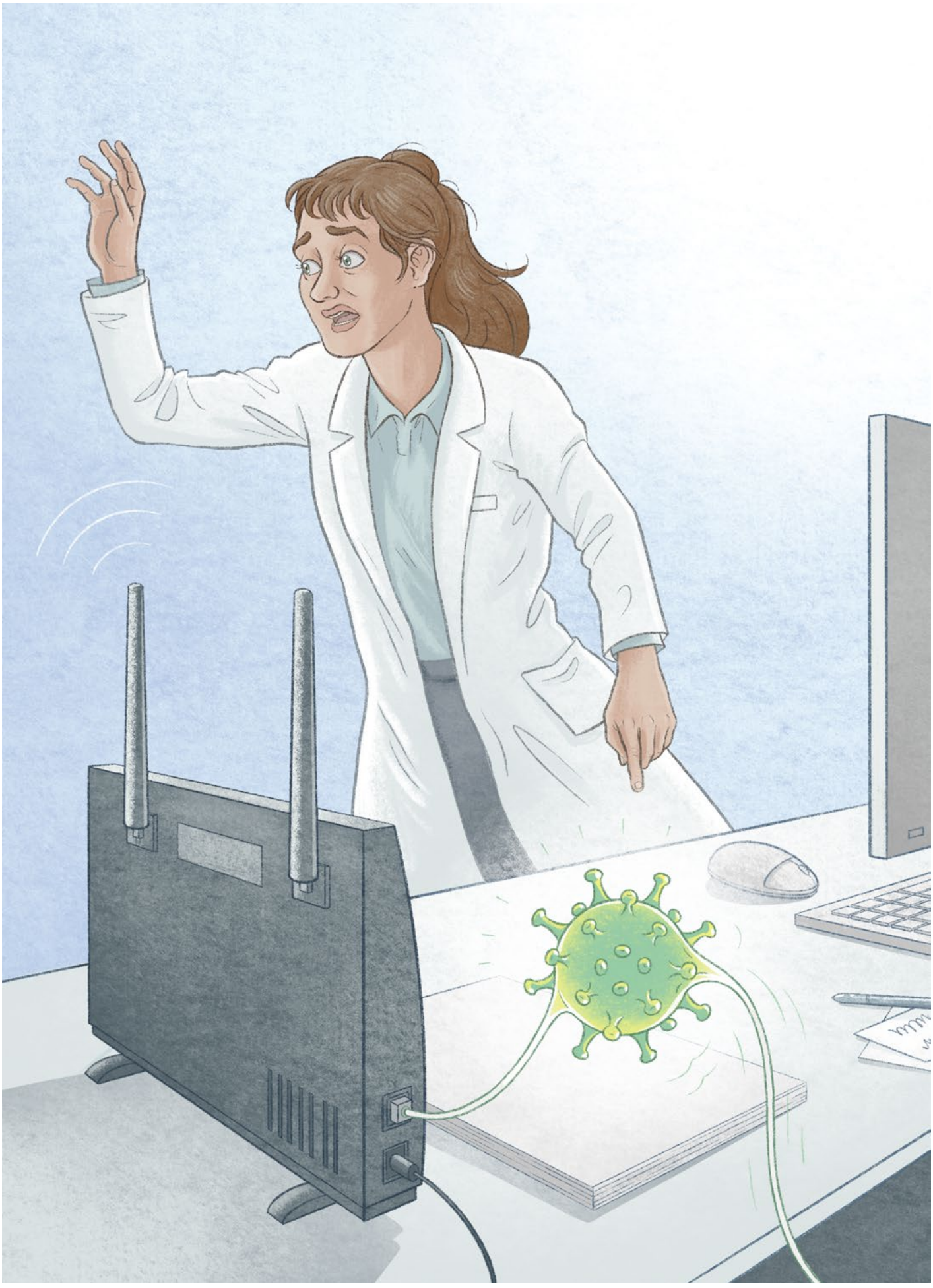
Doch was soll man nun tun, wenn man Opfer einer Cyberattacke geworden ist? Am sichersten ist es, alle Systeme – Computer, Laptops, und so weiter – abzuschalten. Danach schalten Sie auch WLAN-Router aus und trennen das System zusätzlich vom Netzwerk. So können Sie verhindern, dass eine allfällige Schadsoftware weitere Systeme infiziert. Involvieren Sie im Anschluss umgehend Ihren IT-Support, damit dieser Sie beim weiteren Vorgehen unterstützen kann. Dabei ist es wichtig, dass Sie den Vorfall genau schildern: Wurde eine E-Mail geöffnet? Wurde auf einen Link geklickt? Was passierte danach?

Ebenfalls sollten Sie alle Mitarbeitenden Ihrer Praxis informieren, denn vielleicht haben nicht nur Sie die verseuchte E-Mail erhalten … Ihr IT-Support kann dann mit den entsprechenden Vorsichtsmassnahmen (zum Beispiel deaktiviertes Netzwerk) auch die anderen Computer und Mailkonten Ihrer Praxis überprüfen und schädliche Nachrichten aus allen Posteingängen und aus den elektronischen Papierkörben löschen.

Die richtige Backup-Strategie

Und zum Schluss liegt mir noch folgende Botschaft am Herzen: Wer seine Praxis schon im Vorfeld gut auf eine mögliche Cyberattacke vorbereitet, hat im Ernstfall entscheidende Vorteile. Bei einem sogenannten Ransomware-Angriff zum Beispiel werden ein Teil oder auch alle Daten Ihrer Praxis durch den Angreifer verschlüsselt. Im Anschluss fordert dieser dann zum Teil Unsummen an Erpressungsgeld für den Entschlüsselungscode … Haben Sie also bereits im Vorfeld in eine funktionierende Backup-Strategie investiert, die auch Ransomware-Attacken berücksichtigt, wird ein allfälliger Datenverlust nun marginal sein. Ergänzen Sie die Backup-Strategie zudem mit einer guten Endpoint Security (EPS), die auch mit Ransomware klarkommt, haben Sie eine noch bessere Ausgangslage. Durch eine gute Vorbereitung in Kombination mit dem richtigen Verhalten im Ernstfall sind Sie und Ihre Praxis den Cyberkriminellen also keinesfalls schutzlos ausgeliefert.

Lucas Schult
Lucas Schult ist Geschäftsführer (CEO) von HIN. Er schreibt an dieser Stelle regelmässig über digitale Sicherheit.



© Luca Bartulović