Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 04. Oktober 2018

Was tun gegen Schadsoftware?

Die Technologie hilft im Arbeitsalltag, aber sie hat auch gefährliche Nebenwirkungen – zum Beispiel Schadsoftware. HIN-System-Engineer José Nuno Antunes mit wichtigen Tipps und Tricks, um Viren und Co. entgegenzuwirken.

Herr Antunes, man hört diese drei Wörter immer wieder – aber was sind eigentlich Viren, Trojaner und Würmer?

Als Viren, Trojaner und Würmer bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Sie alle gehören zur Gattung Schadsoftware. Solche Software verbreitet sich über E-Mails, Links auf Websites oder USB Sticks. Ist ein Computer von Schadsoftware befallen, kann es sein, dass darauf gespeicherte Dateien nicht mehr vor unberechtigten Zugriffen geschützt sind.

Die Anzahl schädlicher E-Mails und schädlicher Software hat in den letzten Monaten weltweit stark zugenommen. Wie schütze ich mich denn umfassend gegen solche Schadsoftware?

In meiner täglichen Arbeit begegne ich dieser Frage oft. Viele Gesundheitsfachpersonen und Ihre Systeme sind von solchen Angriffen betroffen. Eine grosse Gefahrenquelle sind E-Mails. Es ist essenziell, bei verdächtigen E-Mails nie auf Links zu klicken oder Anhänge zu öffnen. So verbreitet sich Schadsoftware am schnellsten. Allgemein gilt bei verdächtigen E-Mails: seien Sie vorsichtig und löschen Sie die Nachrichten umgehend.

Weiter empfehle ich unseren Kunden immer, für jede Applikation ein unterschiedliches Passwort zu verwenden und die Systeme immer auf dem neuesten Stand zu halten. Updates installiert man am besten immer umgehend – insbesondere, wenn es sich um Sicherheitsupdates handelt.

Ein zusätzlicher Schutz bieten natürlich Virenschutzprogramme. Die Verwendung eines solchen Programmes ist in der heutigen Zeit eigentlich zwingend. Dazu empfehle ich auch immer einen sogenannten Endpoint Service, bei dem Sicherheitsexperten die Systeme «monitoren» und im Ernstfall betroffene Personen umfassend beraten.

Sie haben von schädlichen E-Mails gesprochen. Wie erkenne ich solche überhaupt?

Das Muster bei schädlichen E-Mails ist eigentlich immer ähnlich. Betrüger verfolgen das Ziel, mit solchen E-Mails mentalen Druck beim Empfänger zu erzeugen, beispielsweise durch einen Hinweis auf eine offene Rechnung oder auf Gewinnchancen. Der Empfänger soll dann auf einen Anhang oder einen Link klicken – und sich so die Schadsoftware einfangen.

Passen Sie also auf: Öffnen Sie Anhänge nie, wenn Sie eine direkte Aufforderung dafür erhalten haben und dazu beispielsweise unpersönlich angesprochen werden. Heutige Phishing-Mails – wie man solche schädlichen E-Mails in Fachsprache nennt – sehen täuschend echt aus. Es muss wirklich grosse Vorsicht geboten werden. Ich rate Ihnen, lieber einmal zu oft vorsichtig zu sein.

Eine einfache Möglichkeit, wie Sie prüfen können, wo Links hinführen ist: Fahren Sie mit der Maus über den Link – ohne zu klicken – und schauen Sie, welcher Pfad angezeigt wird.

Und was muss ich tun, wenn ich eine schädliche E-Mail oder schädliche Datei geöffnet habe?

Lassen Sie den Computer von einem aktuellen Virenschutz-Programm prüfen und trennen Sie Ihren Rechner vom lokalen Netzwerk. So können Sie vielleicht verhindern, dass weitere Rechner infiziert werden.

Stellen Sie ausserdem sicher, dass die Nachricht mit dem schädlichen Anhang auf keinem anderen Computer geöffnet wird. Informieren Sie Ihre Arbeitskollegen und löschen Sie die Nachricht aus allen E-Mail-Konten. Setzen Sie sich schlussendlich mit Ihrem IT-Partner in Verbindung.

José Nuno Antunes ist als System Engineer & 2nd Level Supporter zuständig für die IT-Arbeitsplätze der HIN. Zudem unterstützt er Kunden im 2nd Level Support. Nebst einer Ausbildung als Polygraf verfügt er über einen eidgenössischen Fachausweis in Wirtschaftsinformatik und über mehrjährige Berufserfahrung in der IT-Branche.