Checkliste

Wichtige Vorsorgemaßnahmen

- Alle PCs müssen über eine Antivirensoftware verfügen. Die Software muss immer auf dem neuesten Stand sein. Lassen Sie die Antivirensoftware von Ihrem Systembetreuer installieren, damit es nicht zu Unverträglichkeiten mit dem Praxisverwaltungssystem kommt.
- Wenn Sie das Internet nutzen, sollten Sie eine Firewall einsetzen. Sie wehrt Angriffe aus dem Internet ab – wenn sie richtig konfiguriert und stets auf dem neuesten Stand ist. Lassen Sie die Firewall von einem Profi installieren und einstellen. Rufen Sie im Internet nur Ihnen bekannte Seiten auf.
- Versenden und empfangen Sie E-Mails möglichst vom Praxisnetzwerk getrennt, also auf einem separaten PC, Notebook oder Tablet.
- Löschen Sie E-Mails zweifelhafter Absender sofort und leeren Sie anschließend auch den Papierkorb. Klicken Sie nicht auf Dateianhänge und Links, die in das Internet führen. Achtung: Schadsoftware wird bereits aktiviert, wenn Sie das Dokument in der Dateivorschau Ihres E-Mail-Programms ansehen.
- Installieren Sie regelmäßig alle Updates zu Ihrem Betriebssystem und Internetbrowser.
- Führen Sie regelmäßige Datensicherungen durch. Neben den internen Sicherungen sollten Sie Ihre Daten zusätzlich auf externen Datenträgern sichern, denn: Sollte Ihr gesamtes Netzwerk mit einer Schadsoftware infiziert sein, könnten auch die Daten der Sicherung verschlüsselt sein. Benutzen Sie wechselnde Datenträger und bewahren Sie diese an einem sicheren Ort außerhalb der Praxis auf.
- Sensibilisieren Sie Ihr Praxispersonal. Erstellen Sie gegebenenfalls Regeln zum Umgang mit E-Mails und Internet.

Gefälschte E-Mails erkennen

- Seien Sie misstrauisch bei allen E-Mails, die Sie nicht erwartet haben oder die von unbekannten Absendern stammen.
- Achten Sie auf leichte Abwandlungen in der Schreibweise eines Firmen- oder Personennamens.
- Meistens kennen die Absender von Phishing-Mails zwar die E-Mail-Adresse, nicht aber den tatsächlichen Namen eines potenziellen Opfers. Seien Sie daher besonders wachsam bei E-Mails, die mit generischen Ansprachen wie „Sehr geehrte Dame“, „Liebe Kollegen“ oder „Verehrter Kunde“ beginnen.
- Bei E-Mails mit Dateianhängen sollten Sie stets skeptisch sein, besonders bei Dateiendungen wie .exe und .zip. Aber auch Microsoft-Office-Dokumente können Makros mit Schadsoftware enthalten.

Checkliste

- Fahren Sie mit dem Mauszeiger über Links in E-Mails. So wird Ihnen die Ziel-Website des entsprechenden Links angezeigt. Sollte Ihnen diese nicht bekannt vorkommen, nicht dem angekündigten Ziel entsprechen oder unnatürlich lang und kompliziert sein, besteht die Gefahr, dass es sich um den Link zu einer Phishing-Website handelt.

Hilfe, mein PC ist infiziert

- Trennen Sie den Computer sofort vom Strom und allen Netzwerken. So können Sie eventuell verhindern, dass sich die Schadsoftware weiter verbreitet.
- Wenn Sie sich einen sogenannten Verschlüsselungstrojaner eingefangen haben und Sie aufgefordert werden, ein Lösegeld zu zahlen, sollten Sie dies keinesfalls tun. Denn: Erstens garantiert niemand, dass Ihre Daten anschließend tatsächlich wieder verfügbar sind, und zweitens finanzieren Sie damit die Weiterentwicklung von Schadsoftware.
- Wenden Sie sich umgehend an Ihren IT-Dienstleister, da vermutlich das System neu installiert und konfiguriert werden muss. In der Regel müssen infizierte Festplatten ausgetauscht werden. Ihr Dienstleister wird anschließend vorhandene Datensicherungen einspielen, um die Daten wiederherzustellen.
- Stellen Sie eine Strafanzeige bei der Polizei. Die zentrale Anlaufstelle für Cybercrime NRW erreichen Sie per Mail unter *cybercrime.lka@polizei.nrw.de*
- Wenn es sich um eine Datenpanne handelt, von der Patientendaten betroffen sind, müssen Sie der zuständigen Aufsichtsbehörde dies innerhalb von 72 Stunden melden. Sie finden das Formular unter *ldi.nrw.de*
- Haben Sie auf einer Phishing-Website persönliche Information wie Passwörter angegeben, sollten Sie umgehend alle Passwörter und Sicherheitsabfragen ändern. Für den Fall, dass Sie auf einer solchen Seite Kontodaten, Kreditkartennummern oder PINs eingegeben haben, sollten Sie unverzüglich das Kreditinstitut oder den Zahlungsdienstleister informieren und betroffene Konten und Karten sperren lassen.

IT-Berater

Die IT-Beratung unterstützt Ärzte, Psychotherapeuten und Medizinische Fachangestellte bei Fragen rund um den IT-Einsatz in der Praxis.


Claudia Pintaric
Abteilungsleitung


Franz-Josef Eschweiler
Telefon 0211 5970 8197


Britta Lodyga-Gotthardt
Telefon 0211 5970 8279


Sandra Onckels
Telefon 0211 5970 8099


Nicole Elias
Telefon 0211 5970 8188