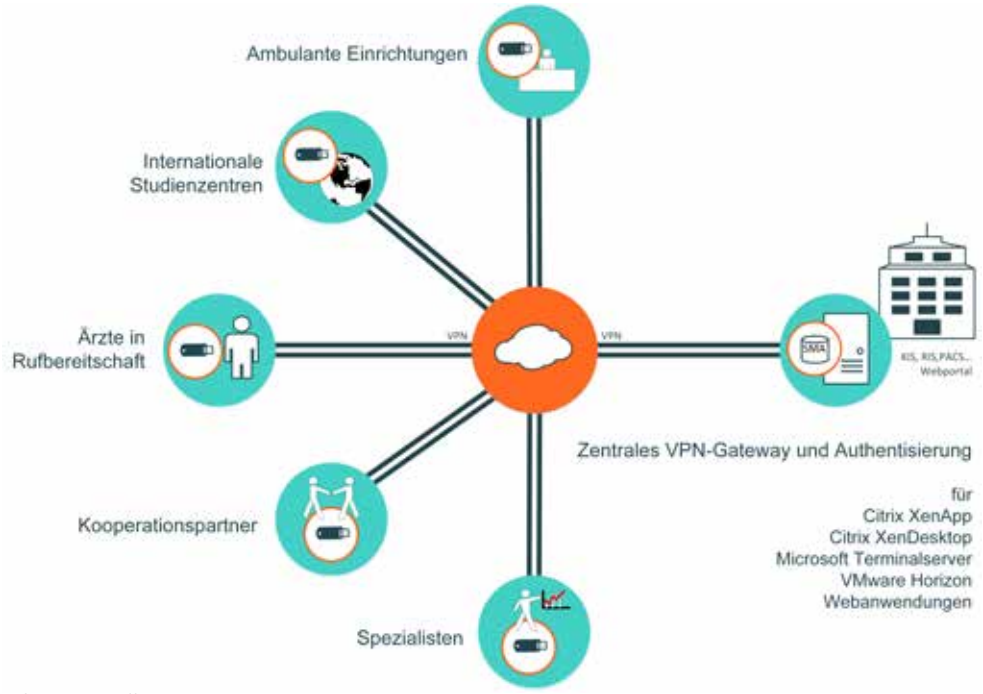
Fernzugriff für das Gesundheitswesen

Sichere Heimarbeitsplätze einrichten
Hochsicherer Zugriff auf Patientendaten von jedem PC

- Hochsicher
- Budgetschonend
- Einfach und flexibel

Fernzugriff für Kiniken und medizinische Einrichtungen

Steigende Belastungen bei Ärzten und Pflegepersonal sowie hoher Kostendruck im Gesundheitswesen erfordern ein flexibles Arbeiten. Dies bedeutet, dass das medizinische Personal einen Zugriff von extern z.B. auf KIS, RIS und PACS benötigt, welcher bisher oft aus Sicherheits- und Kostengründen nicht realisiert wurde.



Fernzugriff für das Gesundheitswesen

Ärzte in Rufbereitschaft

Im Notfall müssen Ärzte und Ärztinnen schnell reagieren können. Oft ist jedoch eine Präsenz im Krankenhaus nicht erforderlich, vielmehr ist die fachliche Diagnose auf Basis von Analysewerten oder Röntgenbildern gefragt. Ein Zugriff auf die notwendigen Patientendaten vom eigenen PC aus spart nicht nur Fahrtkosten, sondern bei Notfällen auch wertvolle Zeit. Zudem entlastet der Wegfall unnötiger Krankenhauspräsenz die Ärzte/Ärztinnen.

Für den Zugriff auf Patientendaten vom heimischen PC aus sind zwei Punkte besonders wichtig: Datenschutz und einfache Nutzung. So muss unter allen Umständen verhindert werden, dass Hacker Zugriff auf sensible Daten erhalten oder gar Bildschirminhalte mitschneiden können. Ebenso dürfen keinerlei Patientendaten auf dem privaten PC abgelegt oder gespeichert werden. Andererseits sind Ärzte keine IT-Experten. Sie benötigen Zugriff vom heimischen PC oder Mac, ohne sich mit der Installation und Konfiguration einer Software auseinandersetzen zu müssen.

Ambulante Einrichtungen

Nicht nur Klinikärzte/-ärztinnen, sondern auch Niedergelassene und sonstige ambulante Einrichtungen benötigen für die Weiterbetreuung der Patienten zunehmend elektronischen Zugriff auf Patientendaten und Krankengeschichten. Ebenso wird ein Zugriff z.B. auf KIS benötigt um OP-Belegpläne einzusehen und Reservierungen vorzunehmen. Der Zugang vom PC des Arztes aus muss benutzerfreundlich sein und ein Zugriff Unbefugter verhindert werden.

Spezialisten

Aufgrund ihrer fachspezifischen Kenntnisse sind spezialisierte Ärzte/Ärztinnen oft für mehrere Kliniken tätig. Dies macht es erforderlich, von extern auf Patientendaten zuzugreifen, um Entwicklungen zu beobachten und bei Bedarf. einzugreifen.

Controller mit weitreichenden Rechten

Controller benötigen aufgrund ihrer bereichsübergreifenden Auswertungen einen umfassenden Zugriff auf alle Systeme. Daher ist dies eine besonders interessante Zielgruppe für mögliche Hacker. Gerade bei einem Zugriff von außen ist es deshalb wichtig für einen hohen Sicherheitslevel zu sorgen.

Heimarbeitsplätze

Im Sinne einer Familienförderung und unter dem Aspekt erfahrene Mitarbeiter an die Einrichtung zu binden, ist es sinnvoll, werdenden Müttern und Eltern mit Kleinkindern eine Vereinbarkeit von Kind und Beruf zu ermöglichen. Unter Sicherstellung einer datenschutzkonformen Nutzung, können auch private PCs ohne Sicherheitsbedenken eingesetzt werden.

Kooperationsnetze

Im Rahmen der allgemeinen Kostensenkungen im Gesundheitswesen gehen Kliniken zunehmend Kooperationen untereinander ein. Damit wird auch eine Vernetzung der IT erforderlich, um auf die Systeme der Partnereinrichtungen zugreifen zu können.

Öffentliche Schulungsräume

Die Weiterbildung von Ärzten/Ärztinnen und Pflegekräften ist ein wichtiger Baustein im Gesundheitswesen. Wenn es um Kliniksoftware geht, wird für die Durchführung der Schulungsmaßnahmen oft auf externe Schulungsräume zurückgegriffen. Das setzt jedoch einen Zugriff auf die entsprechenden Anwendungen voraus, wobei eine zeitraubende Installation und Absicherung auf fremden Schulungsgeräten zu vermeiden ist.

Fernwartung

Kliniken verfügen über eine sehr komplexe Infrastruktur in Sachen IT und Technik. Für die Wartung ist es erforderlich, dass

ECOS SECURE BOOT STICK

die jeweiligen Spezialisten 24/7 hochsicher auf die Anlagen zugreifen können. Aufgrund der vitalen Funktion solcher Anlagen ist ein hoher Schutz vor unbefugten Zugriffen unerlässlich.

DIE PASSENDE LÖSUNG FÜR JEDE ANFORDERUNG

Aus den unterschiedlichen Anforderungen resultieren unterschiedliche Lösungen. Mit Einsatz der ECOS-Technologie können verschiedene Verfahren kombiniert und trotzdem zentral gemanagt werden.

ECOS MOBILE OFFICE STICK – Sicher und flexibel

Für das Arbeiten mit Anwendungen, die eine höhere Sicherheitsstufe voraussetzen, wie z.B. Zuweiserportale, Verwaltungs- oder Pfegedokumentationssysteme, empfiehlt sich zusätzlich zur 2-Faktor-Authentisierung die Ausführung der Client-Software in einer geschützten Umgebung. Der ECOS MOBILE OFFICE STICK kann an einem beliebigen PC oder Mac genutzt werden und enthält sämtliche Software für den Aufbau eines sicheren VPN-Tunnels, sowie die Clients für eine Verbindung zu Citrix, Microsoft Terminalserver, VMware View oder Webanwendungen. Alle Applikationen werden abgeschottet in einer Sandbox ausgeführt.

Der ECOS MOBILE OFFICE STICK dient gleichzeitig als 2 Faktor-Authentisierung und schützt somit vor unautorisierten Zugriffen. Die Nutzung an einem beliebigen PC oder Mac ist völlig instal-

Die passende Lösung für jede Anforderung

lations- und konfigurationsfrei, setzt keine Administratorrechte voraus und hinterlässt keine Spuren auf dem genutzten Gerät.

Adhoc Zugriff per Browser

Für Anwender, welche nur adhoc einen Zugriff auf Daten und Anwendungen benötigen, empfiehlt sich die Nutzung des ECOS VIRTUAL WEB CLIENT (VWC). Über einen Standard-Browser werden ein VPN-Client, und anschließend je nach Anforderung ein ICA-, RDP- oder VMware View-Client geladen, oder auch z.B. ein Browser in einer bestimmten Version. Die Ausführung der Software erfolgt automatisch in einer Sandbox, ohne dass eine Installation oder Konfiguration erforderlich wäre. Bei der Anmeldung wird eine 2-Faktor-Authentisierung per SMS oder OTP-Token unterstützt. Die Lizensierung des ECOS VWC kann nach Named- oder Concurrent-Usern erfolgen. Damit dient der ECOS VWC auch als Fallback, falls ein Anwender seinen ECOS Stick nicht dabei hat.

ECOS SECURE BOOT STICK - Hochsicherer Zugriff

Für einen Zugriff auf Systeme mit sensiblen Patientendaten wie KIS, RIS, PACS, oder auch auf die interne IT, empfiehlt sich der Einsatz des ECOS SECURE BOOT STICK. Mit gestecktem Stick bootet der genutzte PC eine speziell gehärtete ECOS SECURE LINUX-Umgebung. Die lokale Festplatte und das darauf installierte Betriebssystem sind deaktiviert, sodass eventuell vorhandene Schadsoftware gar nicht erst aktiviert wird. Der ECOS SECURE BOOT STICK dient ebenfalls als zertifikatsbasierte 2-Faktor-Authentisierung, da nur die Kombination aus Benutzername, Passwort und dem persönlichen Stick einen Zugriff auf die interne Infrastruktur ermöglicht. Nach erfolgreicher Authentifizierung wird je nach Anforderung ein ICA-, RDP- bzw. VMware View Client oder Browser aufgerufen. Danach befindet sich der Anwender in der von ihm gewohnten Umgebung. Mit dem ECOS SECURE BOOT STICK ist eine 100%ige Trennung zwischen der Nutzung eines PCs für die Einrichtung und der Nutzung für sonstige Zwecke sichergestellt. Datenrückstände oder das Ausspionieren über Trojaner sind ausgeschlossen. Eine integrierte Firewall verhindert zudem Angriffe aus dem gleichen Netz.

Zentrales User- & Rechtemanagement

Alle ECOS-Lösungen werden über ein zentrales Benutzer- und Rechtemanagement verwaltet. So lassen sich Zugriffsrechte auch remote aktualisieren oder sogar entziehen, wenn der Benutzer den Stick möglicherweise noch gar nicht aktiviert hat. Im Falle, dass ein Stick verloren geht, oder von einem ausgeschiedenen Mitarbeiter nicht zurück kommt, kann der Zugang gesperrt und die bestehende Lizenz auf einen neuen Stick übertragen werden.

Vorteile auf einen Blick:

- + Hochsicherer Fernzugriff mit PC oder Mac
- + Geringe Investitionen und Betriebskosten
- + 100%ige Trennung berufliche / private Nutzung
- + Minimale Administration / zentrales Management
- + Einfache Integration in bestehende Infrastruktur
- + Einfach und flexibel – überall nutzbar
- + Datenschutz nach BDSG und BSI-Grundschutz

ECOS TECHNOLOGY GMBH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Tel: +49 (6133) 939-200
Fax: +49 (6133) 939-334
info@ecos.de

114.BF.2016/07.DE.02