KRANKENHAUSGESELLSCHAFT SACHSEN
VERBAND DER KRANKENHAUSTRÄGER IM FREISTAAT SACHSEN

An alle Krankenhausträger
An alle Krankenhausleitungen

2022-01-17

Mitteilung Nr. 034/2022

IT-Sicherheit: Hinweise zum Versand von verschlüsselten E-Mails der Krankenhausgesellschaft Sachsen e. V.

Nahezu täglich können Sie in alltäglichen Medien von Datenpannen und Datendiebstählen lesen. Fremde verschaffen sich Zugang zum internen Unternehmenssystem. Wir möchten Sie in diesem Schreiben auf die sicherheitsrelevanten Maßnahmen, die wir als Krankenhausgesellschaft Sachsen e. V. getroffen haben, informieren. Diese Maßnahmen haben Auswirkungen auf die gemeinsame Kommunikation der Krankenhausgesellschaft Sachsen e. V. mit allen Kommunikationspartnern.

1. Hinweis: Sperrung des Empfangs von Formaten in E-Mail-Anhängen

Die Krankenhausgesellschaft Sachsen e. V. nimmt E-Mail-Anhänge mit folgenden Formaten ab 1. Januar 2022 nicht mehr entgegen. In solchen Fällen wird lediglich der E-Mail-Text zugestellt. Grund für die Sperrung sind Sicherheitserwägungen, da diese Formate u. a. dafür genutzt werden, mit darin versteckter Schadsoftware Computer und Netzwerke anzugreifen und lahmzulegen.

Gesperrte Formate:
.ISP|.JS|.ACE|.MSC|.DLL|.LIB|.APPX|.SYS|.CMD|.VBS|.APPXBUNDLE|.SCR|.MSI|.JSE|.APP|.EX|.ADP|.COM|.VXD|.EX_|.ANI|.CHM|.MST|.DOCM|.JAR|.SHB|.VBE|.MDE|.APK|.NSH|.ADE|.PIF|.LNK|.MSIXBUNDLE|.WSC|.REG|.MSIX|.HTA|.WSH|.BAT|.DMG|.MSP|.CPL|.SC|.ISO|.CAB|.PS1|.EXE|.VB|.INS|.WSF|.doc|.xls|.ppt

Alle Word-/Excel-/PowerPoint-Dateien mit Makros werden weiterhin herausgefiltert.

Krankenhausgesellschaft Sachsen e. V.
Humboldtstraße 2a
04105 Leipzig

T +49 341 98410-0
F +49 341 98410-25

mail@khg-sachsen.de
www.khg-sachsen.de

Deutsche Kreditbank AG Leipzig
IBAN DE77 1203 0000 0018 5047 95
BIC BYLADEM1001

2. Verschlüsselungslösung Global S-MIME/PGP-Encryption

Eine starke Verschlüsselungslösung ist unabdingbar. Wir nutzen eine TLS/S-MIME/PGP-Encryption. Diese sichert die E-Mail-Kommunikation vor unbefugter Veränderung oder Einsicht durch Dritte bis zu unseren Kommunikationspartnern umfassend ab.

Bitte stellen Sie sicher, dass Ihr E-Mail-Programm dieses Verschlüsselungsverfahren beherrscht.

Neben der Übermittlung von einfachen E-Mails (**max. 35 MB)** ohne Verschlüsselung und Signatur an organisations- bzw. personenbezogene E-Mail-Adressen können Sie Ihre E-Mails (**max. 35 MB)** auch verschlüsselt an uns senden.

Wenn Sie eine verschlüsselte Nachricht versenden, so ist deren Inhalt während der Übermittlung für Dritte unlesbar. Das heißt, dass der Nachrichtentext durch ein mathematisches Verfahren mit Hilfe des sogenannten öffentlichen Schlüssels des Empfängers verschlüsselt wurde. Nur mit Hilfe des dazugehörigen privaten Schlüssels, den nur der Empfänger besitzt, kann der Nachrichtentext wieder lesbar gemacht werden.

Voraussetzung für das Versenden verschlüsselter und / oder signierter E-Mails ist die Einbettung des entsprechenden S-MIME in Ihr E-Mail-Programm. Wie Sie dabei vorgehen, ist davon abhängig, welchen Browser und welche E-Mail-Software Sie benutzen.

2.1. Vertrauliche Kommunikation für Empfänger ohne Verschlüsselung

Websafe ermöglicht eine Verschlüsselung von E-Mails sowie eine vertrauliche Zustellung, selbst wenn der Kommunikationspartner keine Möglichkeit besitzt, seinerseits Verschlüsselungsmechanismen einzusetzen.

Erzwungene Verschlüsselung mit Hilfe des Websafes
Der Kommunikationspartner ohne Verschlüsselungstechnologie erhält eine Nachricht zu seinem persönlichen Websafe-Postfach, das https- und passwortgeschützt ist. Alle zukünftigen E-Mails werden verschlüsselt zugestellt und können vom Empfänger über das Websafe-Postfach eingesehen werden.

Um mehr über den Websafe zu erfahren, folgen Sie bitte diesem Link:
https://websafe.cloud-security.net/account/documentation/faq/

3. Datenbereitstellung über die KGS-NextCloud

Die Krankenhausgesellschaft Sachsen e. V. nutzt die KGS-NextCloud, um Ihnen Daten in verschiedenen Formaten bereitzustellen. Somit entfällt der Versand sensibler Daten per E-Mail. Nextcloud ist eine freie Software für das Speichern von Daten auf unseren eigenen Servern.

KGS-Nextcloud verwendet den Industriestandard TLS zur Verschlüsselung von Daten bei der Übertragung. Wir stellen weiterhin sicher, dass die unverschlüsselten Schlüssel nicht auf dem Datenträger selbst gespeichert werden, und im Ruhezustand die Schlüssel durch eine starke Chiffre und Server-seitige Verschlüsselung geschützt sind.

Sämtliche E-Mails der Krankenhausgesellschaft Sachsen e. V. werden automatisch verschlüsselt versendet und mit der entsprechenden Signatur versehen. Der KGS-NextCloud-Service erlaubt Ihnen Zugriff auf alle bereitgestellten Dateien und bietet Ihnen zusätzlich einen Dateiaustausch.

Leider können wir Ihnen wegen der Vielzahl der Möglichkeiten nicht bei der Konfiguration helfen. Bitte wenden Sie sich an den Administrator Ihres Unternehmens (IT-Abteilung), um Hilfe zu erhalten.

Ansprechpartner:
Steffen Gruber
Referent FB Finanzierung und Planung
IT-Verantwortlicher
T +49 341 98410-46
M +49 15120525509
F +49 341 98410-25
gruber@khg-sachsen.de I www.khg-sachsen.de