Absicherung von E-Mail-Accounts

Sehr geehrte Damen und Herren,

durch diese Prüfung möchten wir die Umsetzung des Datenschutzes im Bereich Absicherung der E-Mail-Accounts untersuchen. Die Prüfung erfolgt im gesamten Zuständigkeitsbereich des Katholischen Datenschutzzentrums (d. h. in allen nordrhein-westfälischen (Erz-)Bistümern sowie für den Verband der Diözesen Deutschlands (VDD)).

Die Online-Prüfung kann zu jedem Zeitpunkt zwischengespeichert und zu einem späteren Zeitpunkt fortgesetzt werden. Wenn Sie den Online-Fragebogen über den Menüpunkt "Später fortfahren" verlassen, werden die eingetragenen Antworten gespeichert und beim nächsten Aufruf des Fragebogens wieder angezeigt. Sie haben jederzeit die Möglichkeit, die Beantwortung ab dem Speicherpunkt wieder aufzunehmen und dann auch zu vorhergehenden Frageblöcken der Online-Befragung zurückzuspringen.

Fragen, die mit einem Sternchen (*) gekennzeichnet sind, müssen in jedem Fall beantwortet werden. Es ist nicht erforderlich, dass Sie als Einrichtungsleitung sämtliche Fragen selbst beantworten. Sie können sich für Spezialfragen an die für die Einrichtung zuständigen Stellen wenden. In Betracht kommen hier vor allem IT-Dienstleister, betriebliche Datenschutzbeauftragte, Verwaltungsleitungen und IT-Abteilungen. Der Fragebogen muss innerhalb der im Anschreiben angegebenen Frist abgesendet werden. Nach dem Absenden ist keine Änderung mehr möglich. Nach Ende der Antwortfrist wird der Fragebogen ausgewertet. Für den Fall, dass wir bei der Auswertung weiteren Klärungsbedarf feststellen, werden wir Sie anschreiben.

Wichtiger Hinweis:

Aus Gründen der besseren Lesbarkeit wird nur die männliche Sprachform verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Information zur Verarbeitung personenbezogener Daten gemäß §§ 14, 15, 16 KDG:

Wir verarbeiten Ihre personenbezogenen Daten im erforderlichen Umfang. Weitere Informationen finden Sie unter:

https://www.katholisches-datenschutzzentrum.de/informationspflichten/ (https://www.katholisches-datenschutzzentrum.de/informationspflichten/)

In dieser Umfrage sind 21 Fragen enthalten.

1. Phishing-Awareness und allgemeines Sicherheitsbewusstsein

Trifft die folgende Aussage auf Ihre Einrichtung zu?

Die Mitarbeitenden werden regelmäßig und geeignet zur öffentlich bekannten Bedrohungslage über E-Mail-Angriffsarten geschult. Insbesondere aktuelle Phishing-Kampagnen stehen hierbei im Vordergrund.

Es werden Social-Engineering-Techniken und gefälschte E-Mails, die auch einen Bezug zu bekannter, zum Teil eigener E-Mail-Korrespondenz haben können, dargestellt und Erkennungstechniken zum Aufspüren von Fälschungen erläutert.

Die Geschulten werden dabei instruiert, welches Verhalten präventiv angemessen ist (u. a. kein unbedachter Klick auf Links bzw. Öffnen von Dateien, kein Aktivieren von Makros), aber auch, welche Reaktion zu erfolgen hat, falls der Verdacht einer fehlerhaften Handlung oder eines Sicherheitsproblems besteht.

*

❗ Bitte wählen Sie eine der folgenden Antworten:
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ◯ Ja, diese Aussage trifft auf unsere Organisation zu.
- ◯ Diese Aussage trifft für uns nur teilweise zu.
- ◯ Nein, diese Aussage trifft für uns nicht zu.

Da die vorherige Aussage zu Phishing-Awareness und allgemeinem Sicherheitsbewusstsein in Ihrer Einrichtung nur teilweise zutrifft, teilen Sie uns bitte mit, welche genannten Bereiche zutreffen. Bitte wählen Sie entsprechend aus.

*

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Diese Aussage trifft für uns nur teilweise zu.' bei Frage ' [G00Q01]' (Die Mitarbeitenden werden regelmäßig und geeignet zur öffentlich bekannten Bedrohungslage über E-Mail-Angriffsarten geschult. Insbesondere aktuelle Phishing-Kampagnen stehen hierbei im Vordergrund. Es werden Social-Engineering-Techniken und gefälschte E-Mails, die auch einen Bezug zu bekannter, zum Teil eigener E-Mail-Korrespondenz haben können, dargestellt und Erkennungstechniken zum Aufspüren von Fälschungen erläutert. Die Geschulten werden dabei instruiert, welches Verhalten präventiv angemessen ist (u. a. kein unbedachter Klick auf Links bzw. Öffnen von Dateien, kein Aktivieren von Makros), aber auch, welche Reaktion zu erfolgen hat, falls der Verdacht einer fehlerhaften Handlung oder eines Sicherheitsproblems besteht.)

Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Regelmäßige und passende Schulungen zur Bedrohungslage und zu E-Mail-Angriffsarten finden statt.
- [ ] Es gibt Schulungen oder Informationen zu Phishing-Kampagnen.
- [ ] Social-Engeneering-Techniken und deren Erkennung sind Teil einer Schulung.
- [ ] Angemessenes, präventives Verhalten der Betroffenen wird thematisiert.
- [ ] Reaktion der Mitarbeiter bei einem Sicherheitsproblem oder fehlerhafter Handhabung.

Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Nein, diese Aussage trifft für uns nicht zu.' bei Frage ' [G00Q01]' (Die Mitarbeitenden werden regelmäßig und geeignet zur öffentlich bekannten Bedrohungslage über E-Mail-Angriffsarten geschult. Insbesondere aktuelle Phishing-Kampagnen stehen hierbei im Vordergrund. Es werden Social-Engineering-Techniken und gefälschte E-Mails, die auch einen Bezug zu bekannter, zum Teil eigener E-Mail-Korrespondenz haben können, dargestellt und Erkennungstechniken zum Aufspüren von Fälschungen erläutert. Die Geschulten werden dabei instruiert, welches Verhalten präventiv angemessen ist (u. a. kein unbedachter Klick auf Links bzw. Öffnen von Dateien, kein Aktivieren von Makros), aber auch, welche Reaktion zu erfolgen hat, falls der Verdacht einer fehlerhaften Handlung oder eines Sicherheitsproblems besteht.)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Keine Zeit, kein Geld für Schulungsmaßnahmen.
- [ ] Niemand in der Einrichtung oder beim Träger fühlt sich für Schulungen verantwortlich.
- [ ] Schulungen zu Phishing und zum Sicherheitsbewusstsein sind nicht notwendig.
- [ ] Sonstiges

Bitte erläutern sie Ihre Auswahl "Sonstiges": *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Sonstiges' bei Frage ' [G00Q12]' (Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit.)

Bitte geben Sie Ihre Antwort hier ein:

2. Passwörter, Mehr-Faktor-Authentifizierung und Benutzerverwaltung

Trifft die folgende Aussage auf Ihre Einrichtung zu?

Den Mitarbeitenden steht eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung, um sich an den relevanten Systemen und dem E-Mail-Client anzumelden (z. B. Passwörter mit ausreichender Länge und Komplexität, mehrstufige Authentifizierung).

Dort, wo eine erhöhte Form der Absicherung erforderlich erscheint, werden Zugänge zwingend mit einem zusätzlichen Authentifizierungsfaktor als Ergänzung zum Passwort geschützt. Die Rollen und Berechtigungen zu den E-Mail-Konten werden nach dem Least-Privilege-Prinzip eingerichtet (= nur erforderliche Rechte für die Nutzer).

Richtlinien zur Benutzerverwaltung sind vorhanden und werden regelmäßig geprüft und ggf. angepasst. Zudem werden Nutzerkonten regelmäßig hinsichtlich ihrer Notwendigkeit überprüft (u. a. nicht mehr benötigte E-Mail-Accounts werden stillgelegt, z. B. die von ehemaligen Mitarbeitenden).

*

❗ Bitte wählen Sie eine der folgenden Antworten:
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ◯ Ja, diese Aussage trifft für unsere Organisation zu.
- ◯ Diese Aussage trifft für uns nur teilweise zu.
- ◯ Nein, diese Aussage trifft für uns nicht zu.

Da die vorherige Aussage zu Passwörtern, Mehr-Faktor-Authentifizierung und Benutzerverwaltung in Ihrer Einrichtung nur teilweise zutrifft, teilen Sie uns bitte mit, welche Teilbereiche in Ihrer Einrichtung umgesetzt sind. Bitte wählen Sie entsprechend aus. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Diese Aussage trifft für uns nur teilweise zu.' bei Frage ' [G00Q03]' (Den Mitarbeitenden steht eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung, um sich an den relevanten Systemen und dem E-Mail-Client anzumelden (z. B. Passwörter mit ausreichender Länge und Komplexität, mehrstufige Authentifizierung). Dort, wo eine erhöhte Form der Absicherung erforderlich erscheint, werden Zugänge zwingend mit einem zusätzlichen Authentifizierungsfaktor als Ergänzung zum Passwort geschützt. Die Rollen und Berechtigungen zu den E-Mail-Konten werden nach dem Least-Privilege-Prinzip eingerichtet (= nur erforderliche Rechte für die Nutzer). Richtlinien zur Benutzerverwaltung sind vorhanden und werden regelmäßig geprüft und ggf. angepasst. Zudem werden Nutzerkonten regelmäßig hinsichtlich ihrer Notwendigkeit überprüft (u. a. nicht mehr benötigte E-Mail-Accounts werden stillgelegt, z. B. die von ehemaligen Mitarbeitenden).)

Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Eine Auswahl von sicheren Authentifizierungsverfahren stehen zur Verfügung um sich an relevanten Systemen und dem E-Mail-Client anzumelden.
- [ ] Bei einer erhöhten Form der Absicherung ist der Zugang zwingend mit einem zusätzlichen Authentisierungsfaktor geschützt.
- [ ] Rollen und Berechtigungen zu E-Mail-Konten werden nach dem Least-Privelege-Prinzip eingerichtet.
- [ ] Richtlinien zur Benutzerverwaltung sind vorhanden und werden regelmäßig geprüft und ggf. angepasst.
- [ ] Nutzerkonten werden hinsichtlich ihrer Notwendigkeit überprüft.

Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Nein, diese Aussage trifft für uns nicht zu.' bei Frage ' [G00Q03]' (Den Mitarbeitenden steht eine Auswahl von sicheren Authentifizierungsverfahren zur Verfügung, um sich an den relevanten Systemen und dem E-Mail-Client anzumelden (z. B. Passwörter mit ausreichender Länge und Komplexität, mehrstufige Authentifizierung). Dort, wo eine erhöhte Form der Absicherung erforderlich erscheint, werden Zugänge zwingend mit einem zusätzlichen Authentifizierungsfaktor als Ergänzung zum Passwort geschützt. Die Rollen und Berechtigungen zu den E-Mail-Konten werden nach dem Least-Privilege-Prinzip eingerichtet (= nur erforderliche Rechte für die Nutzer). Richtlinien zur Benutzerverwaltung sind vorhanden und werden regelmäßig geprüft und ggf. angepasst. Zudem werden Nutzerkonten regelmäßig hinsichtlich ihrer Notwendigkeit überprüft (u. a. nicht mehr benötigte E-Mail-Accounts werden stillgelegt, z. B. die von ehemaligen Mitarbeitenden).)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Keine Zeit, kein Geld für Umsetzung der Maßnahmen.
- [ ] Kein Fachpersonal, dass die Maßnahmen umsetzen kann.
- [ ] Die E-Mail-Administration ist ausgelagert und der Dienstleister kann die Maßnahmen nicht umsetzen.
- [ ] Die E-Mail-Administration ist ausgelagert und der Dienstleister wurde nicht mit der Umsetzung beauftragt.
- [ ] Sonstiges

Bitte erläutern Sie Ihre Auswahl "Sonstiges": *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Sonstiges' bei Frage ' [G01Q13]' (Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit.)

Bitte geben Sie Ihre Antwort hier ein:

3. Administrative Pflege der Accounts und Konfiguration

Trifft die folgende Aussage auf Ihre Einrichtung zu?

Die Verwaltung der E-Mail-Postfächer erfolgt strukturiert durch eine Fachabteilung. Durch administrative Einstellungen werden die Clients gezielt konfiguriert und abgesichert (z. B. Verhinderung von vollständigen Downloads ganzer Postfächer). So werden die Default-Einstellungen der verwendeten E-Mail-Software geprüft und durch geeignete Profile organisationsweit kontrolliert.

Einstellungen zu Weiterleitungsregelungen und Abwesenheitsassistenten werden unter Sicherheitsaspekten betrachtet und ggf. eingeschränkt.

Zugänge über Websites wie z. B. Outlook-Web-Access und andere Online-Zugänge zum E-Mail-Client (z. B. Smartphone) werden sicher ausgestaltet. Homeoffice-Faktoren zur sicheren Einwahl werden zudem berücksichtigt (u. a. VPN, eingeschränkte Zugriffsmöglichkeiten per IP-Adressraum).

*

❗ Bitte wählen Sie eine der folgenden Antworten:
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ◯ Ja, diese Aussage trifft für unsere Organisation zu.
- ◯ Diese Aussage trifft für uns nur teilweise zu.
- ◯ Nein, diese Aussage trifft für uns nicht zu.

Da die vorherige Aussage zur Administrativen Pflege der Accounts und deren Konfiguration in Ihrer Einrichtung nur teilweise zutrifft, teilen Sie uns bitte mit, welche Teilbereiche in Ihrer Einrichtung umgesetzt sind. Bitte wählen Sie entsprechend aus. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Diese Aussage trifft für uns nur teilweise zu.' bei Frage ' [G00Q05]' (Die Verwaltung der E-Mail-Postfächer erfolgt strukturiert durch eine Fachabteilung. Durch administrative Einstellungen werden die Clients gezielt konfiguriert und abgesichert (z. B. Verhinderung von vollständigen Downloads ganzer Postfächer). So werden die Default-Einstellungen der verwendeten E-Mail-Software geprüft und durch geeignete Profile organisationsweit kontrolliert. Einstellungen zu Weiterleitungsregelungen und Abwesenheitsassistenten werden unter Sicherheitsaspekten betrachtet und ggf. eingeschränkt. Zugänge über Websites wie z. B. Outlook-Web-Access und andere Online-Zugänge zum E-Mail-Client (z. B. Smartphone) werden sicher ausgestaltet. Homeoffice-Faktoren zur sicheren Einwahl werden zudem berücksichtigt (u. a. VPN, eingeschränkte Zugriffsmöglichkeiten per IP-Adressraum).)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Die Verwaltung der E-Mail-Postfächer erfolgt strukturiert durch eine Fachabteilung.
- [ ] Durch administrative Einstellungen werden die Clients gezielt konfiguriert und abgesichert.
- [ ] Die Default-Einstellungen der verwendeten E-Mail-Software wird geprüft und durch geeignete Profile organisationsweit kontrolliert.
- [ ] Einstellungen zu Weiterleitungsregelungen und Abwesenheitsassistenten werden unter Sicherheitsaspekten betrachtet und ggf. eingeschränkt.
- [ ] Zugänge über Websites wie bspw. Outlook-Web-Access und andere Online-Zugänge (z. B. Smartphone) zum E-Mail-Client werden sicher ausgestaltet.
- [ ] Homeoffice-Faktoren zur sicheren Einwahl werden berücksichtigt. (z. B. VPN)

Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Nein, diese Aussage trifft für uns nicht zu.' bei Frage ' [G00Q05]' (Die Verwaltung der E-Mail-Postfächer erfolgt strukturiert durch eine Fachabteilung. Durch administrative Einstellungen werden die Clients gezielt konfiguriert und abgesichert (z. B. Verhinderung von vollständigen Downloads ganzer Postfächer). So werden die Default-Einstellungen der verwendeten E-Mail-Software geprüft und durch geeignete Profile organisationsweit kontrolliert. Einstellungen zu Weiterleitungsregelungen und Abwesenheitsassistenten werden unter Sicherheitsaspekten betrachtet und ggf. eingeschränkt. Zugänge über Websites wie z. B. Outlook-Web-Access und andere Online-Zugänge zum E-Mail-Client (z. B. Smartphone) werden sicher ausgestaltet. Homeoffice-Faktoren zur sicheren Einwahl werden zudem berücksichtigt (u. a. VPN, eingeschränkte Zugriffsmöglichkeiten per IP-Adressraum).)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Keine Zeit, kein Geld für Umsetzung der Maßnahmen.
- [ ] Kein Fachpersonal, dass die Maßnahmen umsetzen kann.
- [ ] Die E-Mail-Administration ist ausgelagert und der Dienstleister kann die Maßnahmen nicht umsetzen.
- [ ] Die E-Mail-Administration ist ausgelagert und der Dienstleister wurde nicht mit der Umsetzung beauftragt.
- [ ] Sonstiges

Bitte erläutern Sie Ihre Auswahl "Sonstiges": *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Sonstiges' bei Frage ' [G02Q14]' (Da die Ausführungen der vorherigen Aussage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit.)

Bitte geben Sie Ihre Antwort hier ein:

4. Überprüfung des Datenverkehrs

Trifft die folgende Aussage auf Ihre Einrichtung zu?

Aktivitäten am Internetübergangspunkt werden kontrolliert, sodass Aufrufe aus dem internen Netz an bekannte kompromittierte externe Server erkannt werden können (z. B. an der Firewall durch Indicators of Compromise, kurz: IoC).

Es findet hierfür eine Blockierung, Protokollierung und Alarmierung samt regelmäßiger Aktualisierung der IoC-Listen durch geeignete Quellen statt, damit das versehentliche Öffnen schadhafter Websites aus Phishingmails verhindert bzw. erkannt wird.

Zudem besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz, Logging, Überwachung und Absicherung der Logfiles). Firewall-Systeme werden darüber hinaus regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.

*

❗ Bitte wählen Sie eine der folgenden Antworten:
Bitte wählen Sie nur eine der folgenden Antworten aus:

- ◯ Ja, diese Aussage trifft für unsere Organisation zu.
- ◯ Diese Aussage trifft für uns nur teilweise zu.
- ◯ Nein, diese Aussage trifft für uns nicht zu.

Da die vorherige Aussage zur Überprüfung des Datenverkehrs in Ihrer Einrichtung nur teilweise zutrifft, teilen Sie uns bitte mit, welche Teilbereiche in Ihrer Einrichtung umgesetzt sind. Bitte wählen Sie entsprechend aus. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Diese Aussage trifft für uns nur teilweise zu.' bei Frage ' [G00Q07]' (Aktivitäten am Internetübergangspunkt werden kontrolliert, sodass Aufrufe aus dem internen Netz an bekannte kompromittierte externe Server erkannt werden können (z. B. an der Firewall durch Indicators of Compromise, kurz: IoC). Es findet hierfür eine Blockierung, Protokollierung und Alarmierung samt regelmäßiger Aktualisierung der IoC-Listen durch geeignete Quellen statt, damit das versehentliche Öffnen schadhafter Websites aus Phishingmails verhindert bzw. erkannt wird. Zudem besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz, Logging, Überwachung und Absicherung der Logfiles). Firewall-Systeme werden darüber hinaus regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Aufrufe aus dem internen Netz an bekannte kompromittierte externe Server können erkannt werden.
- [ ] Es findet eine Blockierung, Protokollierung und Alarmierung statt.
- [ ] Die IoC-Listen werden regelmäßig durch geeignete Quellen aktualisiert.
- [ ] Es besteht ein Protokollierungs- und Analysekonzept.
- [ ] Firewall-Systeme werden regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.

Da die Ausführungen der vorherigen Frage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Nein, diese Aussage trifft für uns nicht zu.' bei Frage ' [G00Q07]' (Aktivitäten am Internetübergangspunkt werden kontrolliert, sodass Aufrufe aus dem internen Netz an bekannte kompromittierte externe Server erkannt werden können (z. B. an der Firewall durch Indicators of Compromise, kurz: IoC). Es findet hierfür eine Blockierung, Protokollierung und Alarmierung samt regelmäßiger Aktualisierung der IoC-Listen durch geeignete Quellen statt, damit das versehentliche Öffnen schadhafter Websites aus Phishingmails verhindert bzw. erkannt wird. Zudem besteht ein Protokollierungs- und Analysekonzept (Umgang mit Störungsmeldungen, Manipulationsschutz, Logging, Überwachung und Absicherung der Logfiles). Firewall-Systeme werden darüber hinaus regelmäßig hinsichtlich der ordnungsgemäßen Konfiguration überprüft.)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Keine Zeit, kein Geld für Umsetzung der Maßnahmen.
- [ ] Kein Fachpersonal, dass die Maßnahmen umsetzen kann.
- [ ] Die IT-Administration ist ausgelagert und der Dienstleister kann die Maßnahmen nicht umsetzen.
- [ ] Die IT-Administration ist ausgelagert und der Dienstleister wurde nicht mit der Umsetzung beauftragt.
- [ ] Sonstiges

Bitte erläutern Sie Ihre Auswahl "Sonstiges": *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Sonstiges' bei Frage ' [G03Q15]' (Da die Ausführungen der vorherigen Frage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit.)

Bitte geben Sie Ihre Antwort hier ein:

5. Device- und Patchmanagement sowie Backup-Konzept

Trifft die folgende Aussage auf Ihre Einrichtung zu?

Ein vollständiger und aktueller Überblick aller eingesetzten IT-Komponenten des eigenen Betriebs ist vorhanden (IT-Inventar z. B. mit Notebooks aus dem Homeoffice).

Es findet hierfür eine sichere Basiskonfiguration der Systeme und Anwendungen statt. Auch Aspekte zum sicheren mobilen Arbeiten (z. B. im Homeoffice) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet (Anbindung der Telearbeitsplätze und anderer mobiler Clients).

Zur Absicherung der E-Mail-Komponenten besteht ein geregelter Updateprozess inklusive dazugehöriger Dokumentation zur Versionsübersicht. Wichtige Sicherheitsupdates werden unverzüglich eingespielt.

Die eigene IT-Landschaft wird regelmäßig hinsichtlich des Patch-Levels geprüft, insbesondere wegen bekannter Schwachstellen. Darüber hinaus besteht ein wirksames Backup-Konzept zur Sicherung personenbezogener Daten, auch für die Daten aus der E-Mail-Kommunikation.

*

❗ Bitte wählen Sie eine der folgenden Antworten:
Bitte wählen Sie nur eine der folgenden Antworten aus:

◯ Ja, diese Aussage trifft für unsere Organisation zu.
◯ Diese Aussage trifft für uns nur teilweise zu.
◯ Nein, diese Aussage trifft für uns nicht zu.

Da die vorherige Aussage zum Device- und Patchmanagement sowie zum Backup-Konzept in Ihrer Einrichtung nur teilweise zutrifft, teilen Sie uns bitte mit, welche Teilbereiche in Ihrer Einrichtung umgesetzt sind. Bitte wählen Sie entsprechend aus.

*

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Diese Aussage trifft für uns nur teilweise zu.' bei Frage ' [G00Q09]' (Ein vollständiger und aktueller Überblick aller eingesetzten IT-Komponenten des eigenen Betriebs ist vorhanden (IT-Inventar z. B. mit Notebooks aus dem Homeoffice). Es findet hierfür eine sichere Basiskonfiguration der Systeme und Anwendungen statt. Auch Aspekte zum sicheren mobilen Arbeiten (z. B. im Homeoffice) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet (Anbindung der Telearbeitsplätze und anderer mobiler Clients). Zur Absicherung der E-Mail-Komponenten besteht ein geregelter Updateprozess inklusive dazugehöriger Dokumentation zur Versionsübersicht. Wichtige Sicherheitsupdates werden unverzüglich eingespielt. Die eigene IT-Landschaft wird regelmäßig hinsichtlich des Patch-Levels geprüft, insbesondere wegen bekannter Schwachstellen. Darüber hinaus besteht ein wirksames Backup-Konzept zur Sicherung personenbezogener Daten, auch für die Daten aus der E-Mail-Kommunikation.)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

☐ Ein vollständiger und aktueller Überblick aller eingesetzten IT-Komponenten des eigenen Betriebs ist vorhanden.

☐ Es findet eine sichere Basiskonfiguration der Systeme und Anwendungen statt.

☐ Aspekte zum sicheren mobilen Arbeiten (z. B. im Homeoffice) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet.

☐ Zur Absicherung der E-Mail-Komponenten besteht ein geregelter Updateprozess inklusive dazugehöriger Dokumentation zur Versionsübersicht. Wichtige Sicherheitsupdates werden unverzüglich eingespielt.

☐ Die eigene IT-Landschaft wird regelmäßig hinsichtlich des Patch-Levels geprüft, insbesondere wegen bekannter Schwachstellen.

☐ Es besteht ein wirksames Backup-Konzept zur Sicherung personenbezogener Daten, auch für die Daten aus der E-Mail-Kommunikation.

Da die Ausführungen der vorherigen Frage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit. *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Nein, diese Aussage trifft für uns nicht zu.' bei Frage ' [G00Q09]' (Ein vollständiger und aktueller Überblick aller eingesetzten IT-Komponenten des eigenen Betriebs ist vorhanden (IT-Inventar z. B. mit Notebooks aus dem Homeoffice). Es findet hierfür eine sichere Basiskonfiguration der Systeme und Anwendungen statt. Auch Aspekte zum sicheren mobilen Arbeiten (z. B. im Homeoffice) werden in der Behandlung der Systemlandschaft ausreichend beleuchtet (Anbindung der Telearbeitsplätze und anderer mobiler Clients). Zur Absicherung der E-Mail-Komponenten besteht ein geregelter Updateprozess inklusive dazugehöriger Dokumentation zur Versionsübersicht. Wichtige Sicherheitsupdates werden unverzüglich eingespielt. Die eigene IT-Landschaft wird regelmäßig hinsichtlich des Patch-Levels geprüft, insbesondere wegen bekannter Schwachstellen. Darüber hinaus besteht ein wirksames Backup-Konzept zur Sicherung personenbezogener Daten, auch für die Daten aus der E-Mail-Kommunikation.)

❗ Bitte wählen Sie die zutreffenden Antworten aus:
Bitte wählen Sie alle zutreffenden Antworten aus:

- [ ] Keine Zeit, kein Geld für Umsetzung der Maßnahmen.
- [ ] Kein Fachpersonal, dass die Maßnahmen umsetzen kann.
- [ ] Die IT-Administration ist ausgelagert und der Dienstleister kann die Maßnahmen nicht umsetzen.
- [ ] Die IT-Administration ist ausgelagert und der Dienstleister wurde nicht mit der Umsetzung beauftragt.
- [ ] Sonstiges

Bitte erläutern Sie Ihre Auswahl "Sonstiges": *

Beantworten Sie diese Frage nur, wenn folgende Bedingungen erfüllt sind:
Antwort war 'Sonstiges' bei Frage ' [G04Q16]' (Da die Ausführungen der vorherigen Frage in Ihrer Einrichtung nicht zutreffen, teilen Sie uns bitte die Gründe mit.)

Bitte geben Sie Ihre Antwort hier ein:

Kontaktdaten

Für den Fall, dass unsererseits noch weitere Informationen zur Klärung notwendig sind, hinterlassen Sie uns bitte Ihre Kontaktdaten.

Ihre Kontaktdaten:

*

Herzlichen Dank für die Beantwortung unserer Fragen.

Mit freundlichen Grüßen

Katholisches Datenschutzzentrum (KdöR)

Brackeler Hellweg 144

44309 Dortmund

04.08.2023 – 19:00
Übermittlung Ihres ausgefüllten Fragebogens:
Vielen Dank für die Beantwortung des Fragebogens.