Das Magazin für Führungskräfte in Kirchen und kirchlichen Organisationen

www.kviid.de

KVI im DIALOG

4 | November 2020

Finanzen
Ohne Mitgliederorientierung kein nachhaltiges Fundraising - Digitale One-to-One-Kommunikation eröffnet neue Chancen

Facility- & Immobilienmanagement
Rahmenwerk für klimaneutrale Gebäude und Standorte - In Zeiten des voranschreitenden Klimawandels, Teil 3

Management & Organisation
„Ein jegliches hat seine Zeit, und alles Vorhaben unter dem Himmel hat seine Stunde“ (Pred 3,1) - Die Zeit für Verwaltungsreformen ist jetzt!

Informationstechnologien
IT-Risiken in der aktuellen Situation - Wie Sie sich jetzt strukturiert schützen!

KVI Kongress 2020 Special
Alle Erwartungen übertroffen - Der digitale 15. KVI Kongress war mit über 500 Teilnehmenden der bisher erfolgreichste in seiner langjährigen Geschichte

KVI Academy
Wir brauchen Fähigkeiten! - Skills helfen uns - auch persönlich

Personalmanagement
Positives Leadership in Organisationen - Wie manipulativ ist Führung?

IT-RISIKEN

IT-Risiken in der aktuellen Situation - Wie Sie sich jetzt strukturiert schützen!

Ein Beitrag von Carl-Friederich Ehrhardt, Dr. Timo Braun und Patrick Winter

Als gelernter Informatiker und Master of Advanced Studies FHO in Business Information Management hat Carl-Friederich Ehrhardt mehr als zwanzig Jahre Erfahrung im Gesundheitswesen. Besonderer Fokus liegt auf Dokumentationssystemen sowie Informations- und IT-Sicherheit.

Dr. Timo Braun ist seit 2018 im Geschäftsfeld Unternehmensberatung von Curacon tätig. Ein Themenschwerpunkt liegt im Bereich der Informations- und IT-Sicherheit. Hierbei unterstützt er unter anderem Betreiber kritischer Infrastrukturen im Sektor Gesundheit.

Patrick Winter studierte zuerst Betriebswirtschaftslehre. Darauf aufbauend spezialisierte er sich dann auf den Bereich Wirtschaftsinformatik. Die Kernpunkte seiner Arbeit liegen in der Beratung von Trägern im Gesundheits- und Sozialwesen in Bezug auf deren Informationstechnologie.

In allen kirchlichen Einrichtungen, vom Pfarrbüro über die Altenheimverwaltung bis in die Stiftungskonferenz, sind IT-Systeme in Form von Videokonferenzsystemen, Collaboration-Tools und klassischen E-Mail-Systemen in diesen Tagen zu technischen Überbrückern der angebrachten Abstandsgebote geworden.

Doch dies ist nur die Spitze des Eisbergs an IT-Systemen, die sich im Verlauf der letzten Jahre in ihrem Einsatz unverzichtbar gemacht haben.

IT im Gesundheits- und Sozialwesen

Im Gesundheits- und Sozialwesen werden immer mehr vernetzte IT-Systeme eingesetzt, die neue Anwendungsbereiche erschließen und eine steigende Anzahl an IT-Nutzern mit sich ziehen. Dabei wachsen die Anforderungen an die IT-Sicherheit ständig.

Da Organisationen und Mitarbeitern in dieser Branche sensible personenbezogene und gesundheitliche Daten anvertraut werden, sind diese besonderen Anforderungen ausgesetzt.

So wurde ein branchenspezifischer Sicherheitsstandard (B3S) für Krankenhäuser, die als Kritische Infrastruktur gelten, also über 30.000 vollstationäre Fälle pro Jahr vorweisen, erarbeitet und für diese als „Stand der Technik“ verpflichtend definiert.

Doch während nur weniger als zehn Prozent der Krankenhäuser in Deutschland als Kritische Infrastruktur eingestuft sind, kann dieser Sicherheitsstandard auch für kleinere Kliniken und Einrichtungen als Maßstab herangezogen werden.

Hackerangriffe

Wie wichtig die Umsetzung solcher Standards ist, hat jüngst ein irrtümlicher, jedoch erfolgreicher Hackerangriff auf die Uniklinik Düsseldorf gezeigt, bei dem vermutlich russische Hacker 30 Server verschlüsselten und ein Erpresserschreiben hinterließen. Nachdem die Hacker, die eigentlich die Heinrich-Heine-Universität Düsseldorf attackieren wollten, auf ihren Fehler hingewiesen worden waren, gaben diese zwar einen Schlüssel zur Entschlüsselung frei, die Systeme sind aber bis heute nicht voll einsatzbereit.

Auch die Diakonie Mark-Ruhr mit allen Diakoniestationen und einem

Teil der Pflegeheime war bereits Hacker-Angriffen ausgesetzt, die einen Zugriff auf Systeme unmöglich machten, selbst wenn keine sensiblen Patientendaten abgegriffen wurden. Bei der Caritas München verschafften sich Hacker per Phishing-E-Mails Zugang zu Mitarbeiteraccounts, scheiterten aber an dem Versand von Massen-E-Mails.

Doch nicht nur Organisationen der Gesundheits- und Sozialwirtschaft werden durch externe Angreifer bedroht und geschädigt. Auch der Vatikan bleibt nicht immun gegenüber Hackern – so wurde der Heilige Stuhl und das katholische Bistum Hongkong Opfer von vermutlich chinesischen Hackerangriffen, bei denen Mitarbeitern mit Schadsoftware verseuchte Dokumente zugestellt wurden.

IT-Sicherheitsaudit

Um gegenüber externen Bedrohungen aber auch internen Schwachstellen gut aufgestellt zu sein, empfiehlt es sich daher, in regelmäßigen Abständen ein IT-Sicherheitsaudit durchzuführen, welches den aktuellen Status in Bezug auf die IT-Sicherheit überprüft und im Anschluss Ansatzpunkte zur fortwährenden Verbesserung und Erhöhung der IT-Sicherheit aufzeigt.

Dabei stehen die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität im Mittelpunkt. Vertraulichkeit garantiert dabei, Informationen nur einem beschränkten Empfängerkreis zur Verfügung zu stellen. Das Maß, zu welchem ein IT-System über einen bestimmten Zeitraum die an es gestellten Anforderungen erfüllt, beschreibt die Verfügbarkeit, die in dem Beispiel aus Düsseldorf enorm eingeschränkt war.

Letztlich garantiert Integrität die autorisierte Veränderung von Informationen und damit deren Originalität

Abb.: Colourbox

Auch Bistümer, Landeskirchen, Organisationen der Sozialwirtschaft bis hin zum Vatikan werden durch Hackerangriffe bedroht.

und Verlässlichkeit. Dazu werden sowohl organisatorische Abläufe als auch die Sicherheit in den IT-Systemen, Netzen und der Infrastruktur überprüft. Somit ergeben sich aus dem IT-Sicherheitsaudit eine Schutzanalyse, der individuelle Schutzbedarf und ein Schutzentwicklungsplan inkl. Prioritäten.

Ergänzt wird ein IT-Sicherheitsaudit oft durch einen Penetrationstest, bei welchem mögliche Verwundbarkeiten durch Scans der Firewall und Router vom Internet aus (Black-Box-Tests) und die Konfigurationen und Patchstände einzelner Systeme (White-Box-Tests) überprüft werden.

Informationssicherheitsmanagement ist Chefsache

Um die im Rahmen eines IT-Sicherheitsaudits festgestellten Schwachstellen systematisch zu schließen und das Aufkommen neuer zu vermeiden, kann ein Informationssicherheitsmanagementsystem, kurz ISMS, hilfreich sein. Es handelt sich dabei um die Bündelung von Verfahren und Regeln zur Planung, Lenkung und Kontrolle der Informationssicherheit innerhalb einer Organisation.

Diese Systeme sind absichtlich nicht Teil einer jeweiligen IT-Abteilung, um Interessenskonflikte zu vermeiden, die Unterstützung der Leitungsebene zu signalisieren und konzeptionelle Vorgaben machen zu können.

Sicheres Arbeiten auch im Home-Office

Doch selbst wenn die Größe und/oder Komplexität einer Organisation solch ein übergeordnetes Konstrukt nicht erfordert, sollten Veränderungen der IT-Landschaft aus der letzten Zeit aus dem Blickwinkel der IT-Sicherheit noch einmal genauer betrachtet werden. Wie eingangs erwähnt, wurde Digitalisierung im Rahmen der Corona-Krise plötzlich sehr wichtig, sodass Prozesse teilweise verkürzt oder bewusst ausgelassen worden sind.

In vielen Organisationen wurden kurzfristig Home-Office-Lösungen verwirklicht, bei deren Einführung die IT-Sicherheit an manchen Stellen in den Hintergrund getreten ist. So haben einzelne Organisationen fehlende oder unzureichende Regelungen zu Home-Office, die durch die Erarbeitung einer organisationsweiten Dienstvereinbarung geklärt werden sollten.

Durch die vermehrte Nutzung von Endgeräten außerhalb des physischen Organisationsnetzwerks

SCHÜTZEN

wird es zudem essenziell, Firewalls, Virenschutz und die Nutzung von VPNs (zur Tunnelung und Verschlüsselung vertraulichen Informationsaustauschs) auf die aktuellen Anforderungen anzupassen und aufzustocken.

Gleichzeitig sollte sichergestellt werden, dass bei Messenger-Diensten dienstliche von privater Nutzung scharf getrennt wird und datenschutzrechtlich fragwürdige Messenger vermieden werden. Letztlich rundet eine Sensibilisierung der Mitarbeiter über IT-Sicherheit mit Themenschwerpunkten wie dem Umgang mit Organisationsdaten in der Öffentlichkeit, der Wichtigkeit von Backups und der Nutzung von Zwei-Faktor-Authentifizierung ein sicheres Home-Office-Konzept ab.

Sicherer Einsatz von Videokonferenzsystemen

Neben der raschen Einführung von Home-Office-Lösungen haben sich viele Organisationen auch dafür entschieden, bisher als Vor-Ort-Termine stattfindende Zusammenkünfte nun per Videokonferenz abzuhalten.

Diese momentan erzwungene Digitalisierung wird ein Umdenken in vielen Köpfen zurücklassen – so werden Videokonferenzsysteme langfristig eine tragendere Rolle spielen und Organisationen sich überlegen müssen, wie und mit welchem Anbieter Videokonferenzen realisiert werden sollen. Doch diese Entscheidung sollte wohlüberlegt sein. Damit Nutzer dabei nicht alleingelassen werden, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im April 2020 das „Kompendium Videokonferenzsysteme“, kurz KoViKo, vorgestellt. Basierend auf dem IT-Grundschutz-Kompendium definiert dieser Leitfaden detaillierte Anforderungen und unterstützt Anwender von der Planung

Abb.: Colourbox

Es ist sehr wichtig, der IT-Sicherheit den richtigen Stellenwert zuzuschreiben.

über die Beschaffung bis hin zum Betrieb dieser Lösungen.

Bei der Auswahl sollte insbesondere auf eine ausreichende Dimensionierung und Verschlüsselung, den Schutz des Organisationsnetzwerks sowie ein ausdifferenziertes Berechtigungskonzept geachtet werden.

Sicherheit per Verordnung

Für kirchliche Organisationen bestehen neben Vorgaben durch Gesetzgebung und BSI weitere verpflichtende Rahmenwerke, die Maßnahmen zur Gewährleistung von IT-Sicherheit enthalten.

So enthält das vom Verband der Diözesen Deutschlands (VDD) verabschiedete Gesetz über den Kirchlichen Datenschutz (kurz KDG) unter anderem Richtlinien über „Technische und organisatorische Maßnahmen“ (§26 KDG) und zu „Technikgestaltung und Voreinstellungen“ (§27 KDG). Auch das evangelische Kirchenrecht bestimmt nach §27 des EKD-Datenschutzgesetzes, dass verantwortliche Stellen IT-Sicherheit zu gewährleisten haben.

Weiterführend besteht für den Themenkomplex eine eigene Verordnung mit dem sperrigen Namen „Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD)“, in der unter anderem auch auf die Möglichkeit der Bestellung eines gesonderten IT-Sicherheitsbeauftragten eingegangen wird und sich auf die Vorgaben des BSI im IT-Grundschutz bezogen wird. Die Arbeitsgruppe IT-Sicherheitskonzepte der EKD hat für die Umsetzung der ITSVO-EKD bereits Musterkonzepte erarbeitet und zur Verfügung gestellt.

Fazit

Die besonderen Rahmenbedingungen der Corona-Zeit haben die Abhängigkeit von IT-Systemen aufgezeigt und verstärkt. Je höher diese Abhängigkeit jedoch ist, desto verheerender ist ein Ausfall dieser Systeme, sei es durch mutwillige Angreifer, menschliches Fehlverhalten, Umwelteinflüsse oder andere Gefahren.

Umso wichtiger ist es, der IT-Sicherheit den richtigen Stellenwert zuzuschreiben. Durch ein IT-Sicherheitsaudit können bestehende Sicherheitslücken aufgedeckt und systematisch geschlossen werden sowie zukünftige Sicherheitslücken vermieden werden. Ein Informationssicherheitsmanagement basierend auf BSI- bzw. VDD/EKD-Vorgaben untermauert einen strukturierten, langfristigen Umgang mit dem Thema IT-Sicherheit.

Somit kann ein reibungsloser Betrieb auch in Zeiten von Home-Office und Videokonferenzen gewährleistet werden.