



## Cyberisiken für kirchliche Organisationen

Deloitte Dienstleistungen

Ihre Ansprechpartner:



Ralph Noll  
Partner  
[rnoll@deloitte.de](mailto:rnoll@deloitte.de)  
Tel:+49 151 58 07 4682



Dr. Jörg Scheffner  
Director  
[jscheffner@deloitte.de](mailto:jscheffner@deloitte.de)  
Tel:+ 49 160 94 61 5910

## Chancen und Risiken durch fortschreitende Digitalisierung

Die Digitalisierung verschiedenster Bereiche macht auch vor kirchlichen Organisationen nicht halt. Mit zunehmender Digitalisierung und Anbindung an Informationstechnik und das Internet gehen für kirchliche Organisationen jeder Größe Gefahren für die Sicherheit vertraulicher Informationen einher. Besonders gemeinnützige, kirchliche Organisationen waren jüngst Ziele von Cyberkriminalität (insb. Ransomware), hierdurch entstanden zuletzt hohe Lösegeldforderungen und Kosten. Kirchliche und gemeinnützige Organisationen sind verglichen mit Organisationen der Privatwirtschaft wegen ihrer häufig fehlenden Expertise in der Cybersicherheit ein attraktives Ziel von Cyberattacken. Zusätzlich erhöhen das Arbeiten im Homeoffice oder gleichzeitig privat und beruflich genutzte Geräte (BOYD) das Cybersicherheitsrisiko. Daher ist es unerlässlich, auf die Bedrohung durch Cyberangriffe angemessen reagieren zu können und Vorsorgemaßnahmen einzuleiten.

## Unser umfassendes Dienstleistungsangebot

Wir bieten ein breitgefächertes Angebot an Dienstleistungen zum Themenfeld Cybersicherheit in kirchlichen Organisationen an. Die Dienstleistungen reichen von Ransomware Assessments über Asset Discovery & Netzwerkvisualisierungen, Cyber-Reifegrad Schnelltests, Risikoermittlung mit Open Source Intelligence bis hin zur Reaktion auf Cybervorfälle. Unsere Cybersicherheitsexpert:innen verfügen über vielfältige praktische Erfahrungen und bringen diese als Mehrwert in ihr Cybersicherheitsprojekt ein.

## Digitale Sicherheit bei kirchlichen Organisationen

### Besondere Stellung von kirchlichen Organisationen

- Kirchliche Organisationen verpflichten sich auf besondere Weise zum Datenschutz
- Kirchliche Organisationen haben meist ein großes Bedürfnis im Bereich der Cybersicherheit
- Gemeinnützige und kirchliche Organisationen sind in letzter Zeit bevorzugtes Ziel von Cyberangriffen insb. Ransomware

### Möglichkeiten von kirchlichen Organisationen im Bezug auf Cybersicherheit

- Experten mit juristischen, technischen, regulatorischen und wissenschaftlichen Hintergrund hinzuziehen
- Im Sinne der christlichen Botschaft agieren
- Mitglieder binden und Menschen von digitaler Sicherheit überzeugen
- Vertrauen/Reputation in der Gesellschaft durch erhöhte Sicherheitsstandards gewinnen
- Wirtschaftliche Kosten mindern

### Anknüpfungspunkte bei kirchlichen Organisationen

#### Reaktion auf Cybervorfälle

- Je schneller auf einen Cybervorfall reagiert wird, desto besser sind auch die negativen wirtschaftlichen Folgen für die Organisation zu begrenzen

#### Reconnaissance/OSINT-Recherche

- Durch eine proaktive OSINT-Recherche können potentielle Gefahren früh erkannt werden
- Oder als Reaktion auf einen Incident um Schwachstellen zu finden

#### Vorsorgemaßnahmen gegen Ransomware Angriffe

- Schwachstellenidentifikation zur Vorbeugung von Ransomware Angriffen
- Mittels der Simulation von aktuellen Angriffsszenarien

#### Visualisierung des Netzwerkes

- Verbesserung der Netzwerksegmentierung
- Klärung der Verbindungen von Assets

#### Status quo Analysen

- Analyse des Status quo des Cyber-Reifegrades der Organisation



Kompetenz in allen Bereichen der Gefahrenabwehr



Eingehende Erfahrung mit Strategie und technischer Prüfung



Strategieentwicklung und Implementierung



Synergieeffekte mit Allianzen und Partnern

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“), DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter [www.deloitte.com/de/ueberUns](http://www.deloitte.com/de/ueberUns).

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeiterinnen und Mitarbeiter liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: [www.deloitte.com/de](http://www.deloitte.com/de).

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte-Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

## Deloitte Lösungen für Cybersicherheit: Von Vorsorge bis Incident Management

Die Cyberrisiken für kirchliche Organisationen sind vielfältig und vielschichtig. Deloitte ist Vorreiter im Bereich Cybersicherheit und unterstützt Sie in der Umsetzung. Wir bieten ein vielseitiges Spektrum an Dienstleistungen im Cybersicherheitsbereich an, angefangen bei präventiven Maßnahmen wie z.B. Netzwerkvisualisierungen, Ransomware Assessments aber auch Schnelltests über reaktive Leistungen wie Incident Management.

### Die Cybersicherheits-Dienstleistungen von Deloitte umfassen:



#### Asset-discovery und Netzwerkvisualisierung

Tools zur Netzwerkvisualisierung um sich durch verbesserte Netzwerksegmentierung vor Verstößen zu schützen.



#### Ransomware assessment

Bereitstellung leistungsstarker Tools und Simulationen um eine Verbesserung Ihrer Abwehrmaßnahmen herzustellen.



#### Cyber Reifegrad Schnelltest

Feststellung des Status Quo mittels ausführlicher Interviews und technischer Unterstützung, um Verbesserungspotentiale und die Minimierung der Cyberrisiken zu gewährleisten.



#### Risikoermittlung mit open-source intelligence

Erstellung eines digitalen Fußabdrucks der Institution um Schwachstellen aufzudecken und Cyberrisiken kalkulierbarer machen.



#### Incident management

Eine angemessene Reaktion auf Cybervorfälle ist unerlässlich, und bestimmt, inwiefern der Geschäftsbetrieb beeinflusst wird.

Spezialisierte Expertenteams helfen Ihnen bei Cybervorfällen und unterstützen Sie bestmöglich.

## Beispielhaftes Vorgehen: Ransomware Assessment

Ransomware entwickelt und verbreitet sich immer schneller und ist eines der größten Bedrohungen für die Cybersicherheit kirchlicher Organisationen. Der beste Schutz gegen einen Ransomware-Angriff ist die Identifizierung von Lücken, die Bewertung der Verantwortlichkeiten und Prozesse in der Cybersicherheitsinfrastruktur sowie die Verbesserung der Sicherheitsmaßnahmen.

### Tools:

**XM CYBER identifiziert Schwachstellen im Netzwerk, welche für Angriffe z.B. mit Ransomware genutzt werden können wie beispielsweise:**

- Fehlkonfigurationen
- Offene Anmeldedaten
- Schlechtes Benutzerverhalten
- Durch mangelnde IT-Hygiene verursachte Schwachstellen

**Dies erlaubt einen Überblick über das Risiko und eine priorisierte Liste der zu ergreifenden Abhilfemaßnahmen.**

### Funktionen:

- Automatisierte Generierung von umsetzbaren und priorisierten Berichten für Abhilfemaßnahmen und Beseitigung von Schwachstellen
- Sichere Simulation basierend auf realen Benutzeraktionen, die in Echtzeit ausgeführt werden
- Umfassende Berichte über den Cybersicherheitsstatus und die Sicherheitslage der Organisation und Visualisierung der Angriffspfade

### Vorteile:

- Einfache Implementierung und schnelle Amortisation von Sicherheitsinvestitionen sowie eine skalierbare Architektur
- Reduziert das Risiko, welches durch mangelhafte Sicherheitshygiene entsteht
- Optimierung der Nutzung von digitalen und personellen Cyber-Ressourcen

### Weitere Deloitte-Dienstleistungen für kirchliche Organisationen:



Strategische Prozess- und Organisationsberatung



Personal



IT-Strategie