McKinsey & Company

In Kooperation mit

ZELOS Management Consultants

Artikel

Im Fokus: Cybersicherheit in der GKV

Wie Krankenkassen sich wirksam vor Hackerangriffen schützen können

Im Fokus: Cybersicherheit in der GKV

Wie Krankenkassen sich wirksam vor Hackerangriffen schützen können

Von Jan Bartenschlager, Florian Niedermann, Mathis Friesdorf, Benjamin Klein, Matthias Redlich, Andreas Faber und Zoe Zwiebelmann

Im Herbst 2022 wurde Australiens zweitgrößte Krankenversicherung Medibank zum Opfer eines Hackerangriffs: Daten von 9,7 Millionen Versicherten fielen in die Hände von Kriminellen. Als Medibank die Lösegeldforderung verweigerte, begannen sie, sensible Personendaten im Netz zu veröffentlichen – darunter Namen, Adressen und Passnummern bis hin zu medizinischen Befunden und Therapien. Der Fall rüttelte Krankenversicherer in aller Welt auf.

Auch in Deutschland geraten Gesundheitseinrichtungen immer öfter ins Visier von Cyberkriminellen. Mit fatalen Folgen: IT-Systeme fallen aus, Betriebsabläufe und Kommunikationsflüsse werden unterbrochen, medizinische Dokumente nicht übermittelt, Erstattungszahlungen verzögern sich. Solche Hackerangriffe bedeuten nicht nur eine empfindliche Störung des Tagesgeschäfts. Sie sind zur ständigen Bedrohung geworden – für das Gesundheitssystem, die Patientenversorgung und nicht zuletzt für die Versicherten mit ihren persönlichen und medizinischen Daten.

Was die meisten Krankenkassen unterschätzen: Cyberattacken sind viel mehr als nur ein technisches Problem. Sie treffen die gesamte Organisation – Prozesse, Strukturen, Kommunikationsflüsse. Die Lösung des Problems kann deshalb nicht Sache der IT-Funktion allein sein, im Gegenteil: Es bedarf einer übergreifenden Governance und klar geregelter Verantwortlichkeiten, um das Cyberrisiko effektiv in den Griff zu bekommen. Cybersicherheit gehört ganz oben auf die Agenda der Versicherer.

Auch die Regulatoren haben die Gefahr inzwischen erkannt und versuchen, mit immer neuen Verordnungen zur Cybersicherheit gegenzusteuern. So fordert die EU-Richtlinie NIS2, die 2023 in Kraft getreten ist, von den Organisationen unter anderem Lieferkettenanalysen und strengere Meldepflichten – mit Geldstrafen von bis zu 10 Mio. EUR oder 2% des weltweiten Umsatzes bei Verstößen.

Gesetzliche Krankenversicherungen (GKVen) sind als Teil der kritischen Infrastruktur von den erhöhten Anforderungen an die Cybersicherheit besonders betroffen. Umso wichtiger wird es für sie sein, jetzt das Heft in die Hand zu nehmen, wenn sie millionenschwere Schäden abwenden und vor allem die Daten ihrer Versicherten nachhaltig schützen wollen.

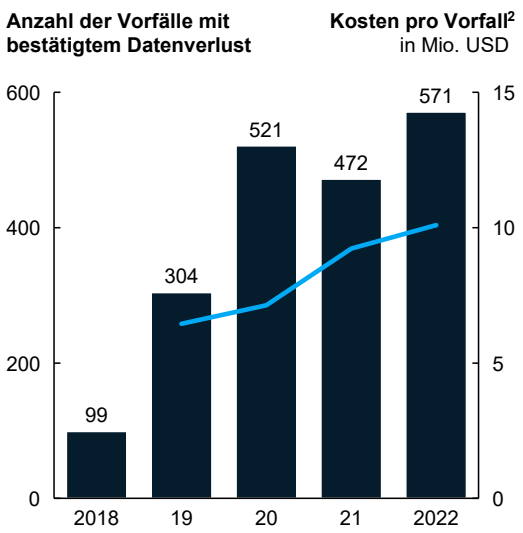
Anstieg der Cyberattacken weltweit um 400%

Gesundheitsorganisationen werden immer häufiger zum Zielobjekt von Cyberkriminalität. Anzahl und Schwere der Attacken nehmen gerade in diesem Sektor seit einigen Jahren sprunghaft zu, wie eine Analyse zeigt: Danach ist dort die Zahl der Cyberangriffe zwischen 2018 und 2022 weltweit um mehr als 400% gestiegen (Abbildung 1). Die Kosten, die dem Gesundheitswesen dadurch entstehen, sind enorm. Pro Vorfall liegen sie durchschnittlich bei rund 10 Mio. USD – höher als in jeder anderen Branche oder Industrie.

Abbildung 1

Die globale Bedrohung von Gesundheitseinrichtungen durch Cyberangriffe wächst rapide

Anzahl und Kosten von Cyberangriffen im globalen Gesundheitssektor[1]



Marktdaten für den Gesundheitssektor 2022 (weltweit)

Nr. 1	im Industrievergleich bei durchschnittlichen Kosten eines Cyberangriffs
10 Mio. USD	durchschnittliche Kosten eines Cyberangriffs mit Datenverlust
95%	aller Attacken haben eine finanzielle Motivation
>75%	der Vorfälle sind Angriffe auf Webanwendungen, Eindringen in Systeme oder eingeschleuste Fehler
38%	der Angriffe erfolgen mit Ransomware (ggü. durchschnittlichen 21% in anderen Industrien)

1. Anzahl der Vorfälle im internationalen Gesundheitssektor (Quelle: Verizon Cybersecurity Solutions); Zahlen illustrieren lediglich die Entwicklung der Bedrohung und entsprechen nicht der Gesamtzahl der Cyberangriffe
2. Durchschnittliche Gesamtkosten eines Vorfalls im Gesundheitssektor über alle Regionen und die Menge der geleakten Daten

Quelle: Verizon DBIR; IBM Security; Presseberichte

Warum ist das Cyberrisiko gerade in letzter Zeit so massiv gewachsen? Die Ursachen hierfür sind auf drei Ebenen zu finden: Erstens vergrößert die zunehmende Digitalisierung der Kassen ihre Angriffsfläche. Zweitens wächst die Zahl der Schwachstellen durch den Einsatz neuer Technologien. Und drittens steigt mit dem technologischen Fortschritt auch die Raffinesse der Angreifenden.

Zunehmende Digitalisierung. GKVen werden immer digitaler. Befeuert durch die Corona-Pandemie erfuhren neue Dienste wie digitale Gesundheitsanwendungen (DiGA) oder elektronische Arbeitsunfähigkeitsbescheinigungen (eAU) einen Boom. Gleichzeitig nimmt die Vernetzung zwischen den Gesundheitseinrichtungen zu. Diese Entwicklungen vergrößern die Angriffsfläche der Versicherer für Cyberkriminelle. Hinzu kommt, dass die sensiblen personenbezogenen Gesundheitsdaten, mit denen die Krankenkassen arbeiten, auf dem Schwarzmarkt zum begehrten Gut geworden sind: Medizinische Informationen, Finanzdaten und Identifikationsmerkmale erzielen dort inzwischen hohe Preise.

Neue Technologien. Auch der Einsatz neuer Technologien und Softwarelösungen kann das Cyberrisiko für die Kassen erhöhen. Vor allem Sicherheitslücken und unsachgemäße Handhabung dienen Kriminellen oft als willkommenes Einfallstor für ihre Angriffe.

Raffinierte Angriffe. Nicht nur die IT-Technologien entwickeln sich weiter, auch die Fähigkeiten derer, die sie knacken. Cyberkriminelle werden immer fortschrittlicher und finanzkräftiger, agieren oft hochprofessionell und haben mitunter mächtige Organisationen hinter sich. Gleichzeitig wächst das Phänomen „Cybercrime as a Service“ (CaaS), das es auch weniger professionellen Einzelakteuren ermöglicht, Tools oder Dienste aus dem cyberkriminellen Umfeld zu erwerben und sie zu nutzen, ohne dass umfassende technische Kenntnisse erforderlich sind.

Datenmissbrauch und Millionenschäden: Die Folgen für Versicherte und Kassen

Cybergefahren schlummern nicht nur in den IT-Systemen der einzelnen Krankenkassen: Digitale Produkte, Services und Gesundheits-Apps bergen ebenfalls Risiken, aber auch Rechenzentren, angeschlossene Leistungserbringer und IT-Dienstleister. Die größte Cyberbedrohung jedoch geht noch immer vom Menschen aus – das zeigen die Erfahrungen aus den jüngsten Vorfällen deutlich. Drei Viertel aller Cyberattacken im Gesundheitssektor erfolgen durch Angriffe auf Webanwendungen, das Eindringen in Systeme oder eingeschleuste Fehler. Zu den häufigsten Methoden zählen Phishing-Attacken, bei denen gefälschte E-Mails und Websites verwendet werden, um an vertrauliche Informationen wie Anmeldedaten zu gelangen.

Für Versicherte können die Folgen dramatisch sein. Bei einem kompletten Systemausfall ist die Kasse oft tagelang – auch telefonisch – nicht erreichbar. Dringende Vorgänge wie Anträge auf Erstattungsleistungen können nicht bearbeitet, Krankengelder nicht ausbezahlt werden. Versicherte geraten so leicht in finanzielle Engpässe, anstehende Reha-Maßnahmen verzögern sich. Langfristig verheerend wirken sich vor allem Datendiebstähle aus: Der Besitz von Namen, Geburtsdaten und Bankverbindungen ermöglicht Cyberkriminellen, unter falscher Identität Verträge abzuschließen oder im großen Stil einzukaufen. Aus der illegalen Veröffentlichung medizinischer Informationen wiederum können den Opfern massive soziale Nachteile erwachsen, z.B. geringere Chancen bei einer Bewerbung. Doch ganz gleich, wie klein oder groß der Schaden ist, den Krankenversicherte durch Cyberattacken erfahren – das Vertrauen zu ihrer Kasse ist danach in jedem Fall erschüttert.

Für die Krankenversicherer ist der Reputationsschaden enorm. Haben sie es doch aus Sicht der Mitglieder versäumt, ihrer Verantwortung für den Datenschutz gerecht zu werden. Die Konsequenzen könnten in einigen Fällen schwerwiegend sein: Digitale Serviceangebote werden möglicherweise kaum noch genutzt; manche Versicherte könnten der Kasse gleich ganz den Rücken kehren. Und selbst wenn es nicht zur Abwanderung kommt, wird es einige Anstrengung kosten, das verlorene Vertrauen wieder zurückzugewinnen.

Die Kassen riskieren aber auch – neben Einschränkungen des operativen Betriebs über Tage oder Wochen – handfeste finanzielle Einbußen: Mögliche Schadenersatzforderungen betroffener Versicherter können in die Millionen gehen. Verstößt eine Kasse außerdem gegen Verordnungen zu Cybersicherheit oder Datenschutz (z.B. NIS2 und DSGVO), drohen ihr zusätzlich empfindliche Strafzahlungen. Zudem fallen bei Cyberangriffen oftmals Kosten für externe Dienstleister an, die helfen, den Schaden zu finden und zu beheben. Hinzu kommen Ausgaben für Krisenkommunikation und notwendige Rechtsberatung – auch sie erreichen nicht selten Millionenhöhe.

Die besten Abwehrstrategien …

Um Angriffe auf ihre IT-Systeme abzuwehren und deren harten Konsequenzen zu entgehen, sollten Krankenversicherer das Thema Cybersicherheit systematisch angehen. Bewährt hat sich ein ganzheitlicher Ansatz aus vorbeugenden und reaktiven Maßnahmen sowie solchen, die auf die gesamte Organisation einwirken. Hier – kurz und kompakt – eine Auswahl wirksamer Abwehrinstrumente:

Vorbeugend. IT-Sicherheitslücken im Geschäftsmodell diagnostizieren und die eigenen Cyberkompetenzen bewerten (Wie cyberfit ist meine Organisation?). Zentrale Systemkomponenten wie Server und Datenbanken schützen durch Installation von Sicherheitssoftware (Patches) und Firewalls. Umfassende Cyberaufklärung in der Organisation betreiben und Belegschaft schulen.

Reaktiv. Cyberattacken anhand interner und externer Quellen frühzeitig erkennen. Notfallpläne erstellen und Fähigkeiten aufbauen zur schnellen Reaktion auf Angriffe. Den Ernstfall mehrfach simulieren. Krisenkommunikation vorbereiten. IT-Sicherheit regelmäßig überprüfen.

Organisatorisch. Sensibilität schaffen für die Relevanz von Cybersicherheit innerhalb der Organisation. Cyber Operating Model etablieren mit definierten Verantwortlichkeiten und klar festgelegter Governance. Weitreichende Cyberstrategie entwickeln inklusive Fahrplan und zugewiesenem Budget.

… und ihre Umsetzung in die Praxis

Keine Frage – der Aufbau umfassender Cyberkompetenzen braucht seine Zeit. Doch insbesondere GKVen sollten schon jetzt dafür sorgen, dass sie zumindest die Basisanforderungen an Cybersicherheit so rasch wie möglich erfüllen. In der Praxis bewährt haben sich fünf elementare Maßnahmen, wie die nachfolgenden Fallbeispiele aus verschiedenen Wirtschaftssektoren zeigen.

1. Diagnose der eigenen Cyberkompetenz
Ein spezielles Diagnoseverfahren (engl.: Maturity oder Capability Assessment) stuft die Cyberkompetenz einer GKV-Organisation ein und bewertet ihre internen Fähigkeiten zur Vorbeugung und Reaktion gegenüber Angriffen. Der Check umfasst auch die Überprüfung von Verantwortlichkeiten und Meldewegen. Am Ende zeigt die Diagnose der Organisation detailliert ihre Kompetenzlücken auf, so dass gezielte Schritte zu ihrer Schließung unternommen werden können. Die Resultate lassen sich zudem mit denen von Wettbewerbern und Best Practices anderer Organisationen vergleichen.

Fallbeispiel Luftfahrtindustrie. Der neue Vorstand eines Luftfahrtunternehmens hat Zweifel an der IT-Sicherheit der Organisation und lässt deshalb den Reifegrad der internen Cyberfähigkeiten untersuchen. Die Diagnose legt erstmals offen, wie viele IT-Systeme im Unternehmen tatsächlich cyberrelevant sind. Und nicht nur das: Die Analyse ergibt auch, dass die bisherigen Überwachungsmechanismen nicht ausreichen, um einen Hackerangriff rechtzeitig zu erkennen. Unterschätzt wurden zudem die Kosten, die eine Attacke verursachen würde: Die Cyberversicherung des Unternehmens weist eine drastische Unterdeckung auf. Anhand dieser Diagnoseresultate kann der Vorstand nun gezielt Maßnahmen ergreifen, um die Sicherheitsmängel zu beheben.

2. Schutz der zentralen Systemkomponenten
Jede GKV sollte die systemkritischen IT-Elemente in der eigenen Wertschöpfungskette kennen und deren Risikostatus bewerten können. Das schließt auch die IT-Dienstleister ein. Hier empfiehlt sich eine gründliche Untersuchung aller internen und angebundenen Systemkomponenten auf ihre Relevanz für die Cybersicherheit.

Fallbeispiel Pharmaindustrie. In einem europäischen Pharmaunternehmen stand Cybersicherheit lange Zeit ganz unten auf der Agenda. Das ändert sich, als die ersten Attacken auf Wettbewerber bekannt werden. Aufgeschreckt durch die Medienberichte, drängt der Konzernvorstand jetzt auf einen schnellen Schutz seiner „Kronjuwelen". Eine Analyse der Wertschöpfungskette fördert die systemkritischsten IT-Elemente, Daten und Dienstleister zutage – und schafft so die Voraussetzung, um ihren Schutzstatus prüfen und weiter verbessern zu können.

3. Simulationen des Ernstfalls
Simulationen schaffen auf plastische Weise ein Bewusstsein für die Cybersicherheit in der eigenen Organisation. Das realistische Nachstellen eines Hackerangriffs hilft dem Leitungsteam, die Risiken zu erkennen und im Ernstfall die richtigen Entscheidungen zu treffen – etwa zu Sofortmaßnahmen, zum Verhalten gegenüber den Kriminellen oder zur öffentlichen Kommunikation. Auch auf der Mitarbeiterebene lassen sich Simulationen durchführen, z.B. Phishing-Kampagnen, die einen nachweislich sensibilisierenden Effekt auf die Beschäftigten haben.

Fallbeispiel Versicherung. In einer großen europäischen Versicherung wird die Simulation einer Ransomware-Attacke zum Augenöffner für die teilnehmenden Führungskräfte. Erstmals wird ihnen klar, welche Prozesse in einem solchen Krisenfall zu durchlaufen und welche Entscheidungen zu treffen sind: Systeme abschalten ja oder nein? Eingehen auf die Lösegeldforderung oder nicht? Wann und auf welchem Weg die Versicherten informieren? Nach der Simulation sind alle überzeugt, dass sie Cybergefahren nun besser einschätzen und Gegenmaßnahmen schneller ergreifen können. Um das Gelernte zu verstetigen, erstellen die Führungskräfte im Anschluss an die Simulation interne Krisenszenarien und setzen ein entsprechendes Programm auf. Drohende Cyberkrisen erzeugen bei ihnen nun einen „Muscle memory"-Effekt – sie sind darauf trainiert, im Ernstfall rasch und richtig zu reagieren.

4. Regelmäßige Sicherheitsprüfung
Cyberresiliente Krankenkassen halten ihre IT-Infrastruktur stets auf dem neuesten Stand. Dazu gehören auch regelmäßige technische Sicherheitsprüfungen. Hier empfehlen sich so genannte Penetrationstests, kurz Pen-Tests. Dabei werden Systeme, Netzwerke und Anwendungen systematisch auf Schwachpunkte und potenzielle Eintrittspunkte für Cyberattacken abgeklopft. Pen-Tests sind spezialisierte Verfahren, die auch von IT-Dienstleistern durchgeführt werden können, wenn die Kompetenz hierfür im eigenen Haus fehlt.

5. Etablierung eines Cyber Operating Model
Wer handelt wie im Ernstfall? Was genau ist wann zu tun? Die Klärung der Verantwortlichkeiten im Hinblick auf Rollen und Prozesse ist essenziell, um ein hohes Maß an Cybersicherheit zu gewährleisten. Ein Cyber Operating Model hilft dabei. Dahinter verbirgt sich der Aufbau einer übergreifenden Sicherheitsfunktion. Parallel dazu werden Governance-Mechanismen geschaffen, die alle internen Abläufe, Zuständigkeiten und Meldewege strukturiert überwachen.

Fallbeispiel Logistikbranche. Ein europäisches Logistikunternehmen mit komplexer IT-Landschaft und zahlreichen Dienstleistern stellt im Zuge einer Cyberattacke empfindliche Defizite fest. Da die Verantwortlichkeiten für den Cyberschutz nicht durchgängig klar festgelegt wurden, ist beim Angriff wertvolle Zeit verloren gegangen. Sechs Monate Zeit nimmt sich daraufhin das Unternehmen, um sein Operating Model zu überarbeiten und Governance-Prozesse zu etablieren. Danach sind die Rollen und Zuständigkeiten an allen Punkten geregelt und die notwendigen Cyberschutzfähigkeiten aufgebaut, sowohl intern als auch bei den IT-Dienstleistern.

Die GKV der Zukunft – digital und cybersicher

Die Praxisbeispiele belegen: Das Cyberrisiko ist allgegenwärtig, auch und gerade für GKVen. Zunehmende Vernetzung, der Einsatz neuer Technologien, wachsende Hackerkompetenzen und immer höhere regulatorische Anforderungen fordern ihren Tribut – Anzahl und Kosten der Cybervorfälle im Gesundheitssektor steigen exponentiell. Dagegen helfen nur Prävention, eine klare Governance, strukturiertes Handeln und der Aufbau von Resilienz.

Klar ist aber auch: Die GKV der Zukunft schreckt nicht vor der Digitalisierung zurück, im Gegenteil. Sie nutzt die Möglichkeiten, die sich bieten, um Technologien wie künstliche Intelligenz, Analytics und Cloud einzusetzen und so eine optimale Gesundheitsversorgung zu gewährleisten. Zugleich schafft sie eine hochmoderne IT-Infrastruktur mit integrierten Sicherheitsmechanismen, um Attacken von außen wirksam vorzubeugen oder sie rechtzeitig zu erkennen und darauf zu reagieren. Sie arbeitet eng mit ihren Versicherten zusammen, damit deren Daten zu jedem Zeitpunkt geschützt sind. Nicht zuletzt verankert sie Cybersicherheit und Datenschutz tief in der Kultur und Strategie ihrer Organisation. Auf einen Nenner gebracht: Die GKV der Zukunft ist digital *und* cybersicher.

Dr. Jan Bartenschlager ist Managing Partner bei ZELOS Management Consultants und leitet dort die Aktivitäten im Gesundheitswesen; **Dr. Florian Niedermann** ist Senior Partner im Stuttgarter Büro von McKinsey; **Dr. Mathis Friesdorf** ist Partner und **Benjamin Klein** Expert Associate Partner im Berliner Büro; **Dr. Matthias Redlich** ist Associate Partner im Frankfurter Büro; **Dr. Andreas Faber** ist Engagement Manager im Kölner Büro; **Zoe Zwiebelmann** ist Beraterin im Hamburger Büro.

Deutscher Healthcare-Sektor
Mai 2023

Designed by Visual Media Europe

www.mckinsey.de

@McKinsey
@McKinsey