IT-Sicherheit @ Gen Re

Gen Re®

A Berkshire Hathaway Company

INHALTSVERZEICHNIS

Die Gen Re steht für finanzielle Sicherheit und Stabilität; wir sorgen dafür, dass unsere Kunden ruhig schlafen können. Was wir versprechen, das halten wir. Und wir versichern unseren Kunden, dass wir uns mit derselben Leidenschaft um die IT-Sicherheit kümmern.

Die stabile IT-Landschaft der Gen Re passt sich den ständig neuen Sicherheitsproblemen und Herausforderungen im IT-Bereich an und trägt damit zur Weiterentwicklung und Anwendung stabiler IT-Steuerungsmechanismen bei. Dadurch können wir unseren Kunden sichere und verlässliche Dienstleistungen unter Einhaltung der IT-Branchenstandards (ISC)^2 CBK bieten. Die IT-Sicherheitsmaßnahmen der Gen Re erfolgen gemäß dem aktuellen Stand der Technik und folgen der Rahmenvereinbarung zur Cybersicherheit des National Institute of Standards and Technology (NIST), ihrer Entsprechung der International Organization for Standardization (ISO) 27001 und orientieren sich an den Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik).

SICHERHEIT UND RISIKOMANAGEMENT

BUSINESS CONTINUITY UND DISASTER RECOVERY PLANNING

Unser betriebliches Kontinuitätsmanagement versetzt uns in die Lage, den Betrieb auch unter widrigen Umständen weiterzuführen. Dies erreichen wir durch entsprechende Belastbarkeitsstrategien, Wiederanlaufziele und Betriebskontinuitätspläne, die wesentlicher Bestandteil einer Risikomanagement-Funktion sind. Der Notfall-Wiederherstellungsplan der Gen Re präzisiert, wie kritische Systeme, Daten, Netzwerke und Telekommunikation wieder instandgesetzt werden. Er wird jährlich aktualisiert und getestet. Die in unseren Betriebskontinuitäts- und Notfall-Wiederherstellungsplänen umrissenen Verfahren sind eigens dazu konzipiert, eine Zusammenarbeit mit unseren Kunden aufrechtzuerhalten.

IT-SICHERHEIT UND RISIKOMANAGEMENT

Die Gen Re hat entsprechend der jeweils geltenden gesetzlichen Bestimmungen interne Unternehmensrichtlinien zum Datenschutz für Nordamerika, Kanada und internationale Geschäftsbeziehungen aufgestellt, die auch Datensicherheitsrichtlinien und Kontrollen beinhalten. Unsere Rechtsabteilung überarbeitet und veröffentlicht diese Richtlinien. Ferner haben wir für jede Unternehmensplattform Datenschutzbeauftragte oder -koordinatoren ernannt. Unsere Dienstleister sind durch vertragliche Vereinbarungen gebunden, deren Einhaltung regelmäßig geprüft wird.

GESETZLICHE VORSCHRIFTEN, RICHTLINIEN, UNTERSUCHUNGEN UND COMPLIANCE

Die IT-Abteilung der Gen Re ergreift geeignete Maßnahmen, um personenbezogene und vertrauliche Daten zu schützen und das geltende Datenschutzrecht umzusetzen. Access Management und Zugangskontrollen dienen der Identifikation, Authentifizierung und Autorisierung, um geschäftliche Anforderungen zu erfüllen und gleichzeitig die Vertraulichkeit, Integrität und Verfügbarkeit zu wahren.

Jedes Jahr erfolgt eine Zertifizierung der autorisierten Nutzer, die ihre Kenntnisse des Verhaltenskodex der Gen Re nachweisen müssen, sofern entsprechende Richtlinien für die Nutzung gelten. Der Zugang zu Daten und Dateiservern der Gen Re ist auf autorisierte Nutzer zur Wahrnehmung von Support-Aufgaben beschränkt. Änderungen der Software-und Server-Konfigurationen unterliegen einem strengen Release-Management-Verfahren, das der vorherigen Genehmigung durch die Geschäftsleitung bedarf.

Am Security-Incident-Management-Prozess der Gen Re sind wichtige Mitarbeiter verschiedener Bereiche der Gen Re beteiligt, die für folgende Aufgaben zuständig sind: Identifizierung, Untersuchung und Begrenzung von Störfällen, Wiederherstellungsmaßnahmen und Berichterstattung nach einem Störfall.

SICHERHEITSBEWERTUNG UND TESTS

Die IT-Systeme und -Prozesse der Gen Re unterliegen regelmäßigen internen und externen Audits. Die technische Sicherheit der Netzwerke, Firewalls und Infrastruktur wird jährlich gründlich geprüft. Hierdurch sollen mögliche Schwachstellen auf System- bzw. Anwendungsebene identifiziert werden, die sich negativ auf die operativen und geschäftlichen Ziele der Gen Re auswirken könnten. Die Gen Re verfügt über ein umfangreiches Security Awareness Program, das das Problembewusstsein der Mitarbeiter schärft und sie darin schult, Risiken zu erkennen und Zwischenfälle zu minimieren; zudem werden die Mitarbeiter mithilfe von realen Gefährdungsszenarien getestet, um ihr Sicherheitsverhalten zu verbessern.

IDENTITÄTS- UND ZUGRIFFSKONTROLLE

Es erhalten nur jene Personen Zugriff auf Daten bzw. die Systeme, die dies zur Erledigung ihrer Aufgaben benötigen. Alle Systeme erfordern eine Authentifizierung über eine eindeutige Benutzer-ID und ein Passwort. Unser Passwort-Standard sieht vor, dass das Passwort komplex ist, in regelmäßigen Abständen geändert wird und Mehrfachverwendung der vergangenen 24 Passwörter ausgeschlossen ist. Bei Beendigung der Zusammenarbeit wird der Zugriff für Benutzer, Lieferanten und autorisierte Berater gesperrt. Die Zugriffsberechtigungen werden regelmäßig vom zuständigen Management geprüft, um sicherzustellen, dass alle Änderungen im Provisioning System erfasst werden, damit nicht mehr notwendige Zugriffsrechte entzogen werden können.

PHYSISCHE UND UMGEBUNGSSICHERHEIT

Sicherheitskontrollen und -verfahren verhindern den unbefugten Zugang zu Anlagen und Systemen der Gen Re. Der Zugang zu den Rechenzentren wird über ein sicheres Schlüsselkartensystem gesteuert. Ausschließlich Personen mit operativem Bedarf erhalten Zugang. Besucher müssen sich an die für das Gebäude geltenden Sicherheitsvorschriften halten.

ASSET SECURITY

In allen Phasen der Softwareentwicklung werden die Asset Security und das optimale Vorgehen durch die IT-Abteilung der Gen Re überprüft. Anbieter von Hard- und Software sowie anderen Technologien werden einer eingehenden Risikoprüfung unterzogen.

VERSCHLÜSSELUNG

Wir schützen die Vertraulichkeit sensibler Daten mittels kryptographischer Lösungen. Dazu verwenden wir die Transport Layer Security (TLS) und eine branchenübliche E-Mail-Verschlüsselung. Tragbare Geräte (wie Notebook-Festplatten, Mobiltelefone und Wechseldatenträger) werden mithilfe einer allgemein anerkannten Technologie verschlüsselt. Festplatten und Wechseldatenträger werden nach dem in den USA geltenden Standard, dem sog. Federal Information Processing Standard (FIPS), Veröffentlichung 140-2, mit dem Advanced Encryption Standard (AES) 256-bit-key verschlüsselt. Für mobile Geräte wird eine symmetrische 80-bit AES-Verschlüsselung mit einem öffentlichen Schlüssel unter Verwendung einer 160-bit Elliptic Curve Cryptography (ECC) genutzt. Digitale Zertifikate kommen auf externen Webseiten zum Einsatz, die die Gen Re für die Kundenkommunikation sowie den Datentransfer nutzt.

SCHUTZ VOR DATENVERLUST

Tools zum Schutz vor Datenverlust sollen sicherstellen, dass bei der Übertragung von sensiblen Daten die Vorschriften zur Informationssicherheit nicht verletzt werden; ferner werden E-Mail-Schutz- und Antispam-Programme sowie eine Filterung externer Webseiten auf geschäftlich relevante Inhalte (web-content filtering) eingesetzt. Auf betriebseigenen Computern ist der Zugriff auf webbasierte private E-Mail-Adressen blockiert und untersagt.

SICHERHEIT BEI DER SOFTWAREENTWICKLUNG

Anwendungssysteme werden erst implementiert, nachdem sie verschiedene Entwicklungsphasen sowie einen Qualitätssicherungs- und Änderungsmanagementprozess durchlaufen haben. Alle Anwender benötigen eine eigene Benutzer-ID und ein Passwort, um sich in firmeneigene Systeme einzuloggen. Bei funktionskritischen Systemen werden mindestens einmal pro Jahr regelmäßige Zugriffskontrollen durchgeführt; dies gilt insbesondere für Systeme, die sensible Informationen, personenbezogene Daten oder Finanzdaten enthalten können. Die für die Verarbeitung der Informationen Verantwortlichen vergeben je nach den betrieblichen Erfordernissen und rechtlichen Vorschriften die entsprechenden Zugriffsrechte.

KOMMUNIKATIONS- UND NETZWERKSICHERHEIT

Die Netzwerk-Infrastruktur der Gen Re ist logisch und physisch voneinander getrennt, wie es die operativen Anforderungen vorsehen. Für Entwicklung und Produktion gibt es separate Umgebungen. Die Gen Re verwendet branchenübliche Antiviren-, und Verschlüsselungsprogramme. Firewalls sollen unbefugte Zugriffe verhindern, während Intrusion Detection Systeme im Netzwerk unberechtigte Zugriffsversuche erkennen sollen.

SICHERHEITSMASSNAHMEN

Es werden regelmäßig Kontrollen durchgeführt und geeignete Maßnahmen ergriffen, um unerlaubte oder verdächtige Aktivitäten festzustellen, ausfindig zu machen und zu untersuchen. Die Gen Re verwendet Tools zur Netzwerk- und Schwachstellenanalyse, um den Zustand des Technologieumfelds zu kontrollieren. Mithilfe von Geräten zur Analyse von Bedrohungen sowie Security Information und Event Management können sicherheitsrelevante Vorfälle schnell in den konkreten Zusammenhang gebracht, analysiert und behoben werden. Bei Zwischenfällen kann das zuständige Team auf einen sorgfältig ausgearbeiteten Incident Response Plan zurückgreifen.

ANWENDUNGEN IM FOKUS

FACWORLD

Die Gen Re richtet ihren Kunden Benutzerkonten für FacWorld Life/Health ein. Nach Unterzeichnung einer Zugangsvereinbarung übermitteln die Kunden der Gen Re eine Liste der Benutzer, die Zugang zu FacWorld Life/Health benötigen. Jeder Benutzer erhält von der Gen Re eine spezifische Benutzer-ID und ein komplexes Passwort, das beim ersten Einloggen geändert werden muss. Auf FacWorld Life/Health können Kunden Dateien, auf die sie selbst und die Gen Re Zugriff haben sollen, gesichert hochladen. Alle hochgeladenen Dateien werden in einer geschützten Datenbank gespeichert. Die hochgeladenen Daten können je nach ihrer Beschaffenheit klassifiziert und segregiert werden. Alle übertragenen Dateien werden automatisch nach drei Monaten gelöscht.

GEN RE CONNECT

In gleicher Weise stellt die Gen Re ihren Kunden nach Unterzeichnung der entsprechenden Zugangsvereinbarung Benutzerkonten für Gen Re Connect zur Verfügung. Die Kunden übermitteln der Gen Re eine Liste der Benutzer, die Zugriff auf Gen Re Connect benötigen. Jeder Benutzer erhält eine eigene Benutzer-ID sowie ein komplexes Passwort. Die Kunden sind verpflichtet, eine Lizenzvereinbarung zu akzeptieren und nach dem ersten Login auf Gen Re Connect ihr Passwort zu ändern.

Gen Re®

Die Gen Re bietet Rückversicherungslösungen für Unternehmen in allen Bereichen der Versicherungswirtschaft, sowohl auf vertraglicher wie auf fakultativer Basis. Als einer der weltweit führenden Rückversicherer ist die Gen Re durch ein Netzwerk von mehr als 40 Niederlassungen in allen wichtigen Rückversicherungsmärkten vertreten.

The difference is…the quality of the promise®

genre.com