Wie GlobalSign seine Umgebung sichert

WHITEPAPER

Bei GlobalSign hat die Sicherheit unserer Dienste und Kundendaten höchste Priorität. Dieses Whitepaper beschreibt allgemein die Praktiken und Kontrollen, die wir einsetzen, um die Integrität, Vertraulichkeit und Verfügbarkeit unserer Umgebung sicherzustellen.

GlobalSigns Ansatz zur Informationssicherheit

Als eine der am längsten in Betrieb befindlichen und größten öffentlich vertrauenswürdigen Zertifizierungsstellen (CAs) verfügt GlobalSign über eine lange Erfolgsgeschichte für die Bereitstellung von hoch sicheren Public Key Infrastructure (PKI) -Lösungen. Informationssicherheit ist ein wichtiges Thema auf Vorstandsebene, und die Geschäftsleitung ist maßgeblich an der Festlegung und Sicherstellung der Umsetzung von Sicherheitsrichtlinien beteiligt, die die Vertraulichkeit, Integrität und Verfügbarkeit der von uns angebotenen Dienste gewährleisten.

Wir haben ein engagiertes weltweites Sicherheits- und Compliance-Team, das für den Betrieb unseres Informationssicherheits-Managementsystems verantwortlich ist. Das System basiert auf dem ISO 27001-Standard und den WebTrust Principles and Criteria for Certification Authorities (Prinzipien und -Kriterien für Zertifizierungsstellen von WebTrust) - dem weltweit anerkannten Regelwerk für den Betrieb einer öffentlich vertrauenswürdigen Zertifizierungsstelle. Unser Managementsystem deckt alle gängigen Bereiche der Informationssicherheit ab, wie z. B.:

- Governance und Strategie der Informationssicherheit
- Kontinuierliche Erstellung von Bedrohungsprofilen, Risikobewertungen und Risikomanagement
- Bewusstsein und Vertrauenswürdigkeit des Personals
- Physikalische und Umgebungssicherheit
- Sicherheitsmaßnahmen und -überwachung
- Zugriffsverwaltung
- Systementwicklung und -pflege
- Incident-Management und Breach Response
- Business Continuity und Disaster Recovery

Abgesehen davon, dass wir die erforderlichen Richtlinien unternehmensweit definiert und verteilt haben, haben wir zum Schutz unserer PKI-Dienste verfahrenstechnische und technische Sicherheitskontrollen implementiert:

- Multi-Faktor-Authentifizierung für alle unsere Anwendungen und Systeme
- Mehrschichtige Netzwerke mit starken Filterkontrollen
- Erweiterte Kontrollen zur Erkennung von Malware
- Air-Gapping von kritischem Schlüsselmaterial wie Root-CA-Schlüsseln
- Zugriffsbeschränkungen in Militärqualität, die den Zugriff auf unsere Rechenzentren beschränken
- Systeme zur Angriffserkennung- und -verhinderung in unseren Büro- und Rechenzentren-Netzwerken
- Festplattenverschlüsselung (Full Disk Encryption, FDE) unserer IT-Ausrüstung
- Wiederkehrende Schwachstellenanalyse (vierteljährlich) und Penetrationstestübungen (jährlich)
- Überprüfung des Quellcodes kritischer Anwendungen
- Schnell reagierendes Patch Management

Neben dem Streben nach höchster Sicherheit für unsere eigene Umgebung, ist GlobalSign ein stolzes und langjähriges Mitglied der wichtigsten, auf Standards ausgerichteten Gremien und Organisationen, wie z. B. das Certificate Authority Browser (CA/B) Forum, das Certificate Authority Security Council (CASC) und das Industrial Internet Consortium (IIC) und ist konform mit dem North American Energy Standards Board (NAESB), dem National Institute of Standards and Technology (NIST) und dem National Cybersecurity Center of Excellence (NCCoE)

Bewusstsein und Vertrauenswürdigkeit der Mitarbeiter

Da sich Bedrohungen der Informationssicherheit schnell entwickeln, müssen dies auch Informationen, Orientierungshilfen und Schulung tun, die wir unseren Mitarbeitern anbieten. Das Bewusstsein für Bedrohungen des Datenschutzes und der Informationssicherheit sicherzustellen ist ein kontinuierlicher Prozess. Dies spiegelt sich bei uns nicht nur in der professionellen Schulung der Mitarbeiter wider, sondern auch in zahlreichen anderen Aktivitäten, um das Bewusstsein im gesamten Unternehmen zu fördern. Um eine ständige Wachsamkeit zu gewährleisten, werden unsere Mitarbeiter immer wieder Phishing-Tests und Simulationen anderer Social-Engineering-Angriffe unterzogen.

GlobalSign überprüft auch die Vertrauenswürdigkeit von Mitarbeitern, die wichtige Funktionen im Unternehmen wahrnehmen. Die Mitarbeiterüberprüfung umfasst Kompetenzen, Ausbildung, frühere Anstellungen, berufliche Referenzen und evtl. kriminelle Vergangenheit (soweit dies in der örtlichen Gerichtsbarkeit des Arbeitnehmers erlaubt ist).

Business Continuity und Disaster Recovery

Unsere Umgebung wurde widerstandsfähig gebaut und kann größeren Umweltkatastrophen, organisierten oder absichtlichen Störungen und den Ausfall von Versorgungseinrichtungen und Diensten standhalten. Unsere Methodik für Business Continuity Management und Disaster Recovery basiert auf dem ISO22301-Standard und beinhaltet Folgendes:

- Business-Impact-Analyse zur Quantifizierung der Geschäftsauswirkungen und zur Festlegung geeigneter Kontinuitätsstrategien
- Abstimmung von Recovery Time Objectives (RTO) und Recovery Point Objectives des Dienstes mit von unseren Kunden gewünschten Key Performance Indicators (KPIs)
- Notfall-Kommunikations- und Benachrichtigungsverfahren zur Information unserer Kunden und anderer vertrauender Parteien
- Kontinuierliche On- und Off-Site-Backups von Informationen
- Jährliche Neubewertung der Business Continuity-Strategie und der Business Continuity-Pläne
- Regelmäßige Tests des Business-Continuity-Plans und der Recovery-Verfahren, um zu gewährleisten, dass Recovery Time und Point Objectives eingehalten werden können
- Dedizierte Recovery-Verfahren und -Pläne für CA-spezifische Disaster wie z. B. Schlüsselkompromittierung

Um eine hohe Verfügbarkeit zu gewährleisten, verfügen wir über Rechenzentren auf der ganzen Welt. Sollte eines dieser Rechenzentren eine Naturkatastrophe oder ein von Menschen verursachtes Ereignis erleben, wechselt der Betrieb automatisch und sofort zu einem anderen Ort. Darüber hinaus unterliegen diese Rechenzentren ebenso wie die Ausstellungsstelle den

Standard-Vorsorgemaßnahmen, wie z. B. mehreren Detektionssystemen, mehreren Verbindungslinien und 24x7x365-Überwachung. Dies bedeutet, dass wir so früh wie möglich auf Ereignisse, die stattfinden oder stattfinden werden, aufmerksam gemacht werden, damit wir auf die geeignetste und effektivste Art und Weise reagieren können.

Datenschutz

GlobalSign respektiert das Recht seiner Kunden auf Datenschutz. Unsere Datenschutzerklärung steht im Einklang mit der Datenschutzgrundverordnung der Europäischen Union (DSGVO) und gilt für das gesamte GlobalSign-Netzwerk und für alle Informationen, die für die Ausstellung der gesamten Palette der GlobalSign-Produkte und -Dienste erhoben werden:

- Wir schützen personenbezogene Daten durch angemessene physikalische, technische und organisatorische Sicherheitsmaßnahmen.
- Wir erbitten eine ausdrückliche Einwilligung für alle personenbezogenen Daten, die betroffene Personen einreichen können.
- Wir erheben keine personenbezogenen Daten, solange sie nicht von der betroffenen Person eingereicht werden.
- Wir verwenden die Daten, die die betroffene Person einreicht, nur für die in unserer Datenschutzerklärung definierten Zwecke.
- Personenbezogene Daten werden nach ihrer Verwendung sicher von uns entsorgt.
- Betroffene haben das Recht, die von GlobalSign gespeicherten personenbezogenen Daten einzusehen und auf Konsistenz zu überprüfen.
- Betroffene haben das Recht, in dem seltenen Fall, dass Fehler in unseren Aufzeichnungen gefunden werden, Daten zu korrigieren.

Compliance und Audit

Um die Compliance zu bewerten und nachzuweisen, unterliegt die Umgebung von GlobalSign mehreren internen und externen Audits, wie z. B.:

- Unabhängige jährliche Audits nach ISAE3000 SOC3 Typ II gegen die branchenführenden Frameworks für Zertifizierungsstellen, durch die wir seit 2001 zertifiziert sind - die zweitlängste Zertifizierung in unserer Branche: WebTrust for Certification Authorities, Extended Validation, SSL Baseline Requirements, Code Signing und EV Code Signing.
- Halbjährliche eIDAS-Konformitätsprüfung anhand der eIDAS-Verordnung und der ETSI-Standards für qualifizierte europäische Vertrauensdiensteanbieter
- Schwachstellen-Scans, die sich auf Netzwerkfilterung, Patch-Management, Konfigurationsmanagement, Anwendungssicherheit und Infrastruktursicherheit konzentrieren
- Kontinuierliche Überwachung der Wirksamkeit von Kontrollen, um die Compliance zu gewährleisten, und dass Sicherheitskontrollen effektiv konzipiert und umgesetzt sind

GlobalSign verfolgt auch aktiv die Zertifizierung nach ISO 27001 (Informationssicherheits-Management) und ISO 22301 (Betriebskontinuitätsmanagement).

Über GlobalSign

GlobalSign ist der führende Anbieter von vertrauenswürdigen Identitäts- und Sicherheitslösungen, die es Unternehmen, Großunternehmen, Cloud-Service-Anbietern und IoT-Innovatoren auf der ganzen Welt ermöglichen, Online-Kommunikation zu sichern, Millionen von verifizierten digitalen Identitäten zu verwalten und Authentifizierung und Verschlüsselung zu automatisieren. Mit Lösungen für hoch skalierte Public Key Infrastructure (PKI) und Identität unterstützt das Unternehmen Milliarden von Geräten, Personen und Dingen innerhalb des Internet of Everything (IoE).

DE: +49 800 7237980
EU: +32 16 89 19 00
UK: +44 1622 766766
verkauf@globalsign.com
www.globalsign.de