WebProof ist sicherheitszertifiziert

Wie sicher ist Ihr Überprüfungsprozess für Dokumente?

Es ist kein Geheimnis, dass wir in einer unsicheren Welt leben. Mit Welt ist sowohl die wirkliche als auch die Cyber-Welt gemeint. Und insbesondere denken wir an die digitale Welt, in der der Großteil unserer Geschäftstätigkeit stattfindet. Auch auf den Überprüfungsprozess von Dokumenten trifft dies uneingeschränkt zu. Bei der Überprüfung von Dokumenten sind Sie unglaublich angreifbar.

Wieso?

Weil Sie dies eventuell auf die herkömmliche und definitiv überholte Art und Weise machen: per E-Mail. Aus Sicherheitsgesichtspunkten ist dies ein reiner Albtraum. Sämtliche Dateien werden irgendwo herumgeschickt, während Sie verzweifelt versuchen, den Überblick über Tausende von E-Mails zur Überprüfung von Dokumenten zu behalten. Können Sie sicherstellen, dass all diese E-Mails auch die angestrebten Sicherheitsstandards erfüllen? Können Sie sicherstellen, dass keine privaten E-Mail-Adressen verwendet werden? Natürlich nicht. Und das ist ein gefundenes Fressen für Cyberkriminelle und Hacker. Gibt es eine Lösung?

Überprüfung von Dokumenten in einer sicheren Umgebung

WebProof ist eine Online-Plattform für Zusammenarbeit und die Überprüfung von Dokumenten, die potenzielle Sicherheitsbedenken als oberste Priorität berücksichtigt. Wenn es um die Sicherheit von WebProofs Kunden geht, gibt es keinen Spielraum für Fehler oder Kompromisse. Schon gewusst? WebProof ist eines der wenigen SaaS- (Software as a Service)-Unternehmen, das die renommierte Sicherheitszertifizierung nach ISO 27001 erreicht hat. Für zusätzliches Gewicht angesichts dieser bemerkenswerten Leistung sorgt die Tatsache, dass sowohl WebProofs Software als auch das Cloud Hosting nach ISO 27001 zertifiziert sind.


QSL
Certificate of Registration
WebProof a/s
ISO Quality Services Limited
ISO 27001 : 2013

WebProofs Sichheitszertifizikat nach ISO 27001

Sicher ist sicher

Mit der Sicherheitszertifizierung nach ISO 27001 bietet WebProof Ihnen die höchste Sicherheitsgarantie, die Sie sich wünschen können. Falls Sie sich fragen, wie sicher WebProof selbst als Unternehmen ist, haben wir auch hier eine erfreuliche Antwort. Hinsichtlich der wirtschaftlichen und finanziellen Stabilität ist WebProof stolzer Inhaber eines AAA-Ratings. Das schaffen nur 2 % aller Unternehmen. Es ist also wirklich außergewöhnlich!

Was bedeutet das für Sie und die Überprüfung von Dokumenten? Zunächst einmal bietet Ihnen die Sicherheitszertifizierung nach ISO 27001 das gute Gefühl, auf unerschütterliche Sicherheit der Spitzenklasse zählen zu können. Zweitens können Sie unsere Dienste und Überprüfungs-Tools beruhigt verwenden, ohne sich zu sorgen, dass sie infolge von finanziellen Schwierigkeiten oder wirtschaftlicher Instabilität eines Tages nicht mehr verfügbar sein könnten.

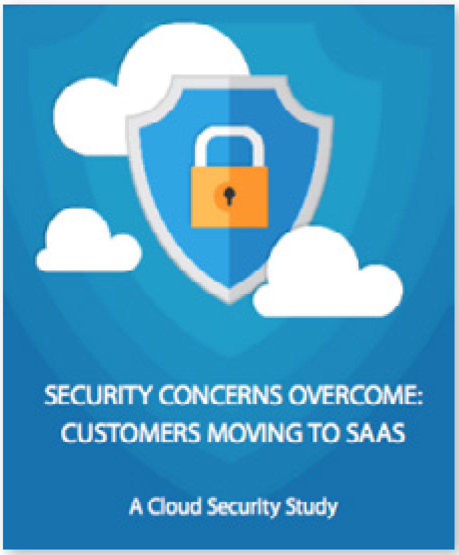
Top-Sicherheitsstandards für Top-Kunden

Wenn Sie mehr über die Sicherheitszertifizierung nach ISO 27001 erfahren möchten, können Sie dazu im Internet recherchieren oder sich jederzeit an unseren Kundenservice wenden. So können Sie sich selbst davon überzeugen, wie schwierig und komplex es ist, diese Art von Zertifizierung zu erhalten. Sie werden es zu schätzen wissen, eine Möglichkeit zur Überprüfung Ihrer Dokumente zu haben und sich keine Sorgen machen zu müssen, ob Ihre sensiblen Unternehmensdaten gefährdet oder Ihre Dokumente durch Sicherheitslücken bedroht sind.

Was ist ADOBEs Ansatz für SaaS-Sicherheit?

Heutzutage sind mehr als 94 % aller Unternehmen stark abhängig von SaaS (Software-as-a-Service). Laut einer Studie der Info-Tech Research Group vertraut die überwältigende Mehrheit der IT-Manager der Sicherheit von SaaS mehr als ihren eigenen Sicherheitslösungen und -ressourcen. Als Adobe-Partner verfolgt WebProof alle Sicherheitstrends aufmerksam und überprüft täglich die Vertrauenswürdigkeit der SaaS-Sicherheit. Hier finden Sie den SaaS-Sicherheitsbericht der Info-Tech Research Group, damit Sie sich ihn gleich näher ansehen können. Adobe legt seinen Partnern ausdrücklich nahe, Sicherheitszertifikate zu erwerben und die höchsten SaaS-Sicherheitsstandards anzulegen.

WebProof wird seiner Strategie treu bleiben, nur auf die renommiertesten und vertrauenswürdigsten Zertifizierungen der Branche zu setzen. Wir sorgen dafür, dass die Überarbeitung Ihrer Dokumente stets effizient, wirtschaftlich und vor allem: sicher sein wird!



Was ist die ISO 27001-Zertifizierung für Informationssicherheits-Management?

Ein Informationssicherheits-Managementsystem ist ein systematischer und proaktiver Ansatz zur wirksamen Steuerung von Risiken, die die Sicherheit der vertraulichen Informationen eines Unternehmens bedrohen. Das System fördert das effiziente Management sensibler Unternehmensinformationen, erkennt Sicherheitsrisiken und stellt so sicher, dass diese Informationen angemessen vor potenziellen Bedrohungen geschützt sind.
Dies umfasst Gebäudesicherheit, Mitarbeiter, Prozesse und IT-Systeme. So können Sie sicher sein, dass WebProof in Bezug auf die Sicherung seiner eigenen Daten seine Integrität behält.

Das ISO 27001-Zertifikat von WebProof kann hier heruntergeladen werden: WebProofs ISO 27001-Zertifikat

Die Normenfamilie ISO/IEC 27000 hilft Organisationen beim Schutz ihrer Informationsbestände.
Die Umsetzung dieser Normenfamilie unterstützt Ihre Organisation bei der Verwaltung der Sicherheit von Werten wie Finanzinformationen, geistigem Eigentum, Mitarbeiterdaten oder Informationen, die Ihnen von Dritten anvertraut wurden. ISO/IEC 27001 ist die bekannteste Norm in der Familie. Sie definiert die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS).

Was ist ein ISMS?

Ein ISMS ist ein systematischer Ansatz für das Management von sensiblen Unternehmensinformationen, das die Sicherheit gewährleistet. Es umfasst Mitarbeiter, Prozesse und IT-Systeme und verwendet ein Verfahren für das Risikomanagement. Es kann kleine, mittlere und große Unternehmen aller Branchen dabei unterstützen, Informationsbestände zu schützen.
Über die Online Browsing Platform können Sie frei verfügbare Abschnitte derISO/IEC 27001:2013 einsehen. Wenn Sie die gesamte Norm erwerben möchten, suchen Sie bitte den ISO-Shop auf.

Wie auch bei anderen ISO-Normen für Managementsysteme ist eine Zertifizierung nach ISO/IEC 27001 optional und nicht vorgeschrieben. Manche Organisationen entscheiden sich für die Umsetzung der Norm, um von den darin vorgeschlagenen Best Practices zu profitieren. Andere lassen sich darüber hinaus auch zertifizieren, um Kunden zuzusichern, dass die Empfehlungen eingehalten werden. ISO führt keine Zertifizierung durch.

Erfahren Sie mehr über die ISO-Normen für Managementsysteme.

WebProof verwendet Amazon aufgrund von Cloud-Sicherheit

WebProof hat vor Jahren mehr als 100 Millionen Dateien aus dem eigenen Serverpark in die Amazon Cloud migriert. Dies geschah nicht aus Kostengründen, sondern vielmehr aufgrund der alle Aspekte umfassenden höheren Sicherheit, wie beispielsweise Lastverteilung und Clustering.

WebProof verwendet Amazon Web Services (AWS) als Cloud-Zentrum, da dies weltweit der sicherste Hosting-Partner ist. Da sich das Hosting-Zentrum in Irland befindet, unterliegt es den EU-Bestimmungen zum Datenschutz. Darüber hinaus verfügt AWS über ein ISO 27001-Zertifikat für das Informationssicherheits-Management.

Certificate

Certificate number: 2013- 009
Certified by EY CertifyPoint since:
November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

headquartered in Seattle, Washington, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: November 11, 2013
Re-issue date of certificate: December 4, 2015
Expiration date of certificate: November 12, 2016

EY CertifyPoint will, according to the certification agreement (dated October 23, 2014), perform surveillance audits and acknowledges the certificate until the expiration date of the certificate.

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in Statement of Applicability, approved on October 22, 2015.*

Drs. R. Toppen RA
Director EY CertifyPoint

1/3 © Copyrights with regard to this document reside with Ernst & Young CertifyPoint B.V. headquartered at Antonio Vivaldistraat 150, 1083 HP Amsterdam, The Netherlands. All rights reserved. DIGITAL COPY

Beschreibung der ISO 27001-Erfüllung durch Amazon

ISO 27001 ist eine Sicherheitsmanagementnorm. Sie definiert Best Practices zum Sicherheitsmanagement und legt aufbauend darauf umfassende Sicherheitskontrollen fest. Voraussetzung für die Zertifizierung ist die Entwicklung und Umsetzung eines strengen Sicherheitsprogramms. Dazu gehört die Entwicklung und Umsetzung eines Informationssicherheits-Managementsystems (ISMS), mit dem festlegt wird, wie AWS fortwährend ein umfassendes und ganzheitliches Sicherheitsmanagement sicherstellt. Diese weithin anerkannte internationale Sicherheitsnorm legt fest, dass Organisationen:

- alle Risiken für die Informationssicherheit systematisch bewerten, wobei die Auswirkungen von Bedrohungen und Schwachstellen aus dem Unternehmen selbst berücksichtigt werden.
- ein umfassendes Spektrum an Informationssicherheitskontrollen und weiteren Formen des Risikomanagements entwickeln und einführen, um Sicherheitsrisiken, die sich aus dem Unternehmen selbst und der Architektur ergeben, entgegenzuwirken.
- einen übergreifenden Managementprozess implementieren, um sicherzustellen, dass die Informationssicherheitskontrollen unseren Anforderungen an die Informationssicherheit dauerhaft gerecht werden.

Die Umsetzung und Erfüllung der Normen ISO 27001, 27017 und 27018 seitens AWS zeugt von einem Bekenntnis zur Informationssicherheit, das sich auf alle Ebenen des Unternehmens erstreckt. Durch Auditierung durch einen unabhängigen Prüfer wird bestätigt, dass AWS die Kriterien der ISO 27001 erfüllt. Die Einhaltung dieser international anerkannten Normen und Geschäftspraktiken ist der Nachweis dafür, dass AWS über ein umfassendes Sicherheitsprogramm verfügt, das mit den anerkannten Best Practices der Branche übereinstimmt.

Das ISO 27001-Zertifikat von AWS kann hier heruntergeladen werden.

Elemente und Aspekte von WebProofs Sicherheitsprogramm für Ihre Datensicherheit

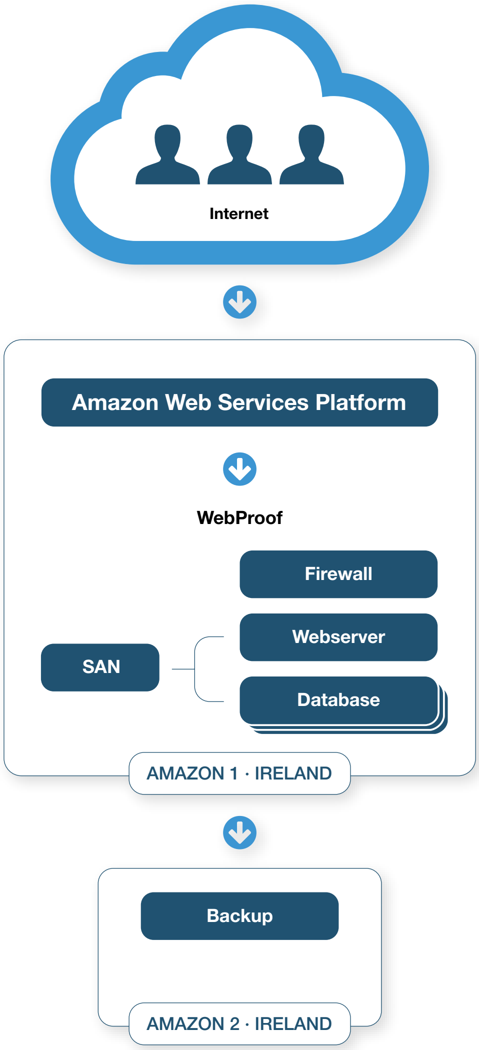
Sicherheitsaspekte können grob in folgende Bereiche unterteilt werden: Sicherheit des Cloud-Hosting-Zentrums; Anwendungssicherheit; Benutzersicherheit; Sicherheit von Entwicklung/Debug und Produktion; Sicherheit der Entwicklungsumgebung; und Sicherheit auf Organisationsebene. All diese Bereiche sind gleichwertig wichtig, denn jedes System ist nur so stark wie seine schwächste Komponente. Dies macht die ISO 27001 so relevant, denn sie ist eine sichere Methode, um zu gewährleisten, dass die Informationssicherheit stets auf dem aktuellen Stand ist. Jeder in unserem Unternehmen ist in das Informationssicherheits-Managementsystem nach ISO 27001 eingebunden.

Sowohl die WebProof-Software als auch unsere Organisation arbeiten nach den Prinzipien der LEAN-Theorie. Die ISO 27001 stellt hier eine natürliche Erweiterung dar, die auf zwei Regeln basiert: systematisches Follow-up – Verbesserung, Follow-up – Verbesserung usw.

Wir werden hier nicht alle Details preisgeben, die zur Sicherung Ihrer Daten beitragen. Doch im Folgenden finden Sie Antworten auf einige der Fragen, die uns häufig gestellt werden (siehe nächste Seite).

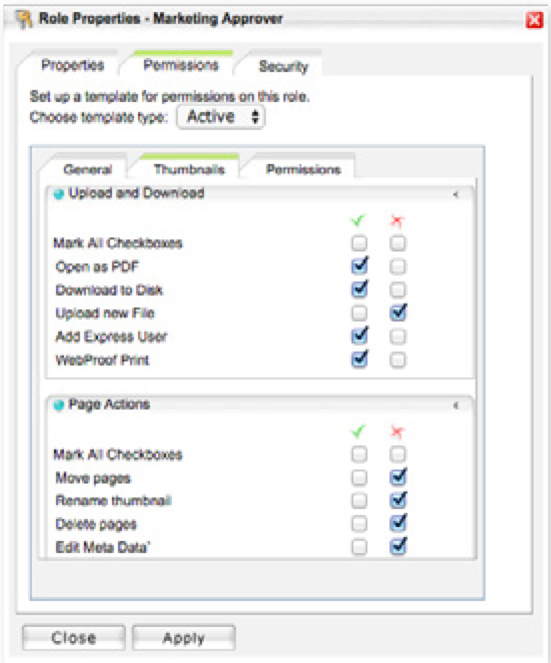
Typische häufig gestellte Fragen (FAQ)

- *Cloud-Hosting – wir verwenden Amazon Web Services, die die höchstmögliche Sicherheit auf der Welt bieten. Der Dienst entspricht den EU-Vorschriften zum Datenschutz. AWS ist sowohl nach ISO 27001 als auch nach ISO 9001 zertifiziert. Das Rechenzentrum erfüllt alle der weltweit gebräuchlichsten Normen und Sicherheitsprotokolle. Unser Rechenzentrum ist Amazon Irland. Bei der Nutzung von AWS werden Sie niemals Geschwindigkeitsbegrenzungen oder Ausfälle der Internetverbindungen zu spüren bekommen, denn AWS verfügt über mehrere Cloud-Standorte und Telekommunikationsanbieter. Nachstehend finden Sie weitere Einzelheiten zu Amazon. Für noch mehr Informationen besuchen Sie Amazon Web Service.*
- *Der Notfallwiederherstellungsplan ist schnell und simpel. Er basiert auf unserem geclusterten Aufbau aus physisch getrennten Servern, die als sofortiges Backup fungieren.*

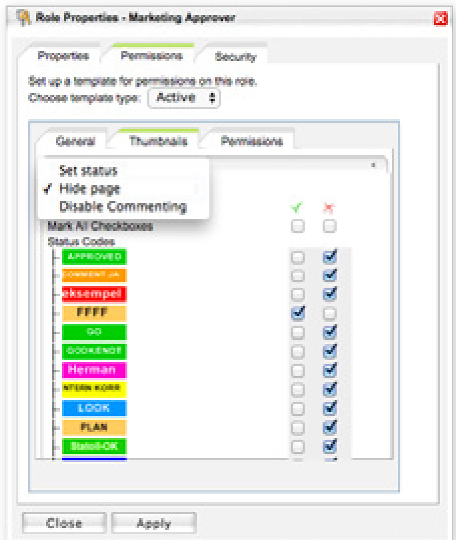


- *In allen Serverparks spielen Sicherheitsbedenken eine große Rolle: Spiegelung, Clustering, Firewall-Sicherheit usw.*
- *Alle Server haben ein eigenes Master-Passwort.*
- *Es handelt sich um ein vollständig redundantes Setup ohne Single Point of Failure im Hardware- oder Netzwerkaufbau.*
- *Kundendaten und Datenbanken werden auf Serverebene getrennt gespeichert. Eine Vermischung der Daten ist daher nicht möglich, nicht einmal im Fall von menschlichem Versagen.*
- *WebProof unterstützt HTTPS, FTP-S, TLS usw.*
- *WebProof lässt mindestens vierteljährlich einen vollständigen Sicherheits-Penetrationstest durch unabhängige Dritte ausführen.*
- *WebProof ist zu 100 % Web-basiert. Sie benötigen nur einen Browser. Kein Java, keine Plugins, keine Add-ons und noch nicht einmal Flash!*

- *WebProof verfügt über eine fortschrittliche Lösung für das Rechte- und Berechtigungsmanagement. So erhält stets nur der richtige Benutzer Zugriff auf die korrekte Version.*



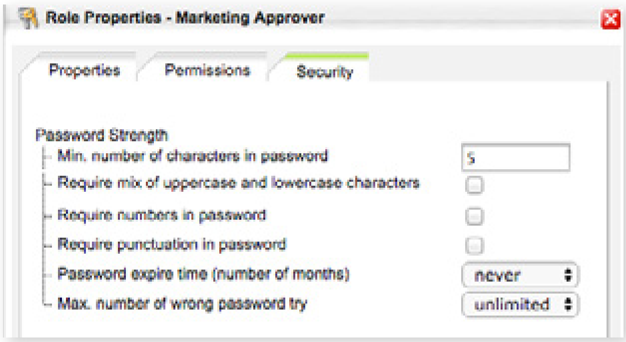
- *Kunden können bestimmte Seiten in einem Projekt ausblenden. Dies wird üblicherweise für die Finanzseiten in Geschäftsberichten börsennotierter Unternehmen oder für vertrauliche unveröffentlichte Informationen verwendet.*



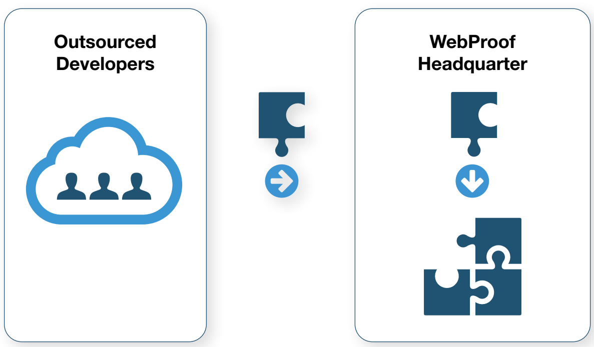
- *Geschützt gegen den PDF-Wurm-Virus (Benutzer öffnen immer nur ein JPG und müssen keine PDF-Datei herunterladen).*
- *Daten können bis zu eine Woche lang wiederhergestellt werden. Wenn Sie ein Projekt aus Versehen löschen, können wir es sofort wiederherstellen.*
- *Mit WebProof können Versionsgeschichten und gespeicherte Daten solange in den Archiven aufbewahrt werden, wie Sie möchten.*
- *Die Verfügbarkeitsgarantie beträgt 99,9 % über drei Monate – das sind weniger als fünf Minuten Ausfallzeit je 24 Stunden. Sollte diese Garantie wider Erwarten nicht erfüllt werden, so erhalten Sie für die zusätzliche Ausfallzeit eine Rückerstattung.*
- *Geplante Wartungszeiten für Hard- und Software finden ausschließlich am Wochenende statt, also zu einer Zeit, an der statistisch gesehen wenig Traffic verzeichnet wird, um beim Kunden für so wenig Unterbrechung wie möglich zu sorgen.*

Typische häufig gestellte Fragen (FAQ)

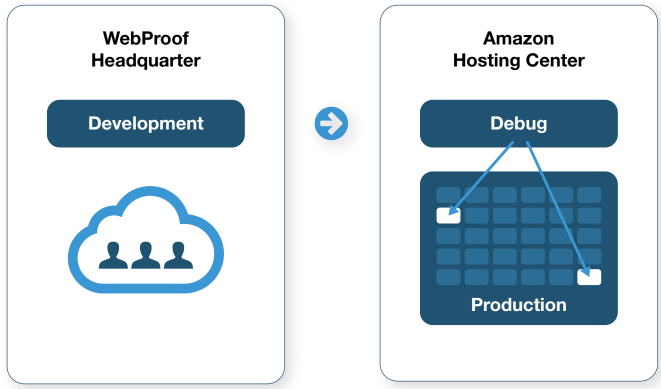
- *Innerhalb unserer Firewalls werden die Systeme durch Netzwerkadressenübersetzung, IP-Adressierung, usw. geschützt.*
- *Kennwörter werden verschlüsselt und per Hash-Algorithmus gesichert und können von niemandem eingesehen werden – nicht einmal von WebProof.*
- *Sie können sich für ein 2048-Bit-SSL-Zertifikat anmelden.*
- *Die Sicherheitseinstellungen für Benutzerkennwörter können durch den WebProof-Administrator des Kunden angepasst werden; als Mindestanforderungen gelten jedoch Benutzername und ein 5-stelliges Kennwort. Dieses wird als MD5-Hash mit Salt gespeichert: Das bedeutet, weder WebProof noch irgendjemand anderes kann es entschlüsseln. Nur wenn Benutzer den korrekten Benutzernamen und das Kennwort kennen, können sie sich anmelden.*



- *Alle Benutzerdaten werden aufgezeichnet, einschließlich der IP usw.*
- *Auf Wunsch fügen wir als erweiterte Kennwort-Lösung einen SMS-Code hinzu, wenn Benutzer sich anmelden und wenn besondere Statuscodes verwendet werden. Dies könnte beispielsweise für den Status GENEHMIGT gelten. Dies entspricht der US-amerikanischen CFR Part 11, einer ähnlichen Sicherheitszertifizierung wie die ISO 27001.*
- *Alle Kundendaten in der WebProof-Übersicht können als XML-Daten exportiert werden. Darüber hinaus können Lageberichte für alle Aktivitäten direkt oder für Sortierzwecke erstellt werden.*
- *Kunden können IP-Einschränkungen für ihre Lösung einrichten. Dies bedeutet, dass sich nur Benutzer mit bestimmten IP-Adressen anmelden können.*
- *Die Sicherheit unserer Systeme ist bereits von den IT-Abteilungen unserer größten Kunden wie LEGO, COOP, ICA und anderen großen bekannten Marken genehmigt worden.*
- *Die vielen Entwickler von WebProof befinden sich in verschiedenen Ländern und verfügen über hoch qualifizierte Entwicklungsressourcen, die nur sehr wenige Menschen weltweit besitzen. Aus genau diesem Grund geht Wissen für uns vor Standort. Unsere externen Entwickler haben eingeschränkten Zugriff auf die Entwicklungs-Server am Hauptsitz. Auf Kundendaten haben sie keinerlei Zugriff.*



- *WebProofs interne Entwickler befinden sich in unserem Hauptsitz. Sie stellen alle Funktionen in WebProof zusammen und sorgen dafür, dass sie den WebProof-Standards entsprechen. WebProof ist immer im Besitz von und hat volle Kontrolle über den Quellcode aller entwickelten Teile. Nur drei Personen am Hauptsitz von WebProof können auf die Produktionssysteme des Kunden zugreifen – unter der Voraussetzung, dass Sie dies genehmigen und den Zugriff erteilen. Niemand kann logischen Zugriff auf Kundendaten erlangen, außer dann, wenn Benutzername und Kennwort vom Kunden preisgegeben werden.*
  Kennwörter werden nie im Klartext gespeichert, sondern stets als Hash-Version mit Salt, sodass eine Entschlüsselung unmöglich ist.
- *Die Entwicklung der WebProof-Software erfolgt an einem anderen physischen Standort als dem Hosting-Zentrum. Die beiden Standorte sind vollkommen unabhängig voneinander.*



- *Sobald ein Update an einem Entwicklungsstandort fertiggestellt ist, wird die Debug-Umgebung am Hosting-Standort aktualisiert. Für den Debug-Standort gilt derselbe Aufbau wie für die Produktion. Er ist jedoch von der Produktion getrennt, für den Fall, dass Probleme auftreten sollten.*
- *Wenn das Update vom Debugger getestet und freigegeben wurde, wird es in die Produktion verschoben und auf einem oder mehreren Live-Systemen aktualisiert.*
- *Jedes Live-System in der Produktion hat seinen eigenen privaten Container für Daten, Datenbanken und Web. Updates können also zum Praxistest auf einigen wenigen Systemen eingesetzt werden, ohne dass weitere Live-Systeme beeinträchtigt werden. Sobald das Update für eine gewisse Zeit stabil läuft, wird es auf alle Live-Systeme angewendet. Wie lange es in dieser isolierten Produktionsumgebung läuft, hängt von der Komplexität des Updates ab.*
- *Ein kleiner Bugfix muss nur ein paar Stunden getestet werden, doch größere Updates erfordern Tests von bis zu mehreren Wochen. Ein sofortiges Zurückspielen ist jederzeit möglich, falls das Update unerwünschte Auswirkungen hat.*
- *Alle internen und externen Mitarbeiter von WebProof unterzeichnen eine strenge Vertraulichkeitserklärung und akzeptieren hohe Anforderungen an Identifizierung und Verifizierung.*
- *Wir setzen Multifaktor-Authentifizierung (MFA) ein. Das bedeutet, dass wir nur Zugang zum System erhalten, wenn wir einen Benutzernamen, ein sicheres Passwort und einen persönlichen einmaligen Code eingeben, der sich minütlich ändert.*