Firmenübersicht

eb-Qual ist qualifizierter Partner führender Hersteller im Schweizer Markt und ist auf ICT-Sicherheit & Netzwerk-Services im privaten und öffentlichen Sektor spezialisiert

Der im Jahr 2002 gegründete ICT-Dienstleister eb-Qual AG ist auf die Beratung, Planung, Konzeption und Implementierung anspruchsvoller ICT-Security- und Netzwerklösungen spezialisiert. Das in Fribourg und Kloten/ZH domizilierte Unternehmen beschäftigt qualifizierte und erfahrene Mitarbeitende und setzt im Sinne eines hohen Qualitäts-Standards auf Produkte und Lösungen weltweit führender Hersteller. Zu den Kunden zählen anspruchsvolle, mittelgrosse Unternehmen, ebenso wie global operierende Konzerne. Das inhabergeführte, unabhängige und kontinuierlich wachsende Unternehmen eb-Qual zählt zu den führenden IT-Security- und Netzwerkspezialisten der Schweiz.

Unsere Mission

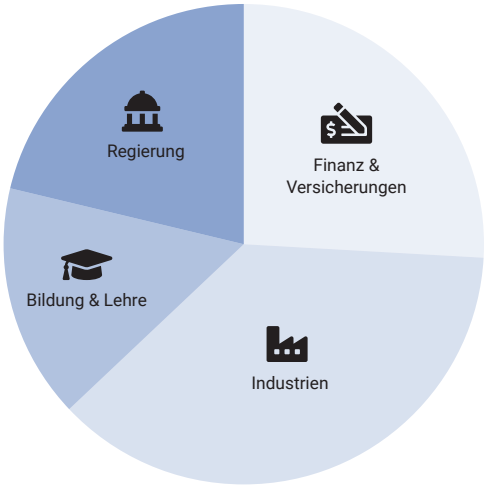
Die Mission von eb-Qual besteht darin, Unternehmen auf die potenziellen Risiken von Cyber-Angriffen aufmerksam zu machen und die Sicherheit und Effizienz ihrer IT-Infrastrukturen mithilfe von marktführenden Lösungen und des Fachwissens unserer qualifizierten Experten zu verbessern.

Die Qualität steht für uns im Mittelpunkt

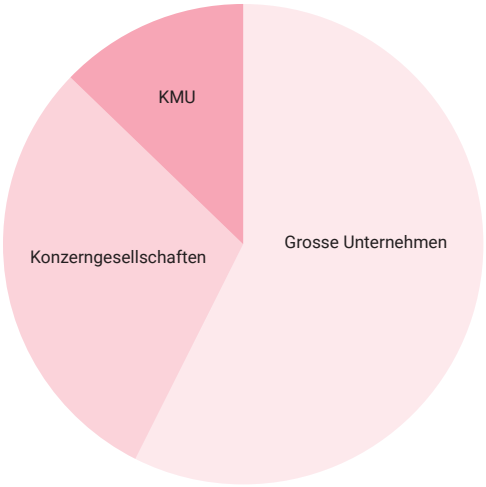
eb-Qual hat höchste Anforderungen an die Qualität ihrer Lösungen und Dienstleistungen, die nur mit ausgewählten Produktpartnern, kompetenten Mitarbeitern und jahrelanger Erfahrung möglich sind. Unterstützt von effizienzsteigernden und qualitätssichernden Massnahmen und Prozessen, garantieren wir optimale Kundenzufriedenheit und sind stolz auf unsere langjährigen Kundenbeziehungen, sowohl bei nationalen Unternehmen wie auch bei global agierenden Konzerngesellschaften. Dafür muss die Qualität unserer Dienstleitungen höchsten Ansprüchen genügen. Dafür werden unsere Cyber Security Engineers, Account Manager und Helpdesk Mitarbeiter durch kontinuierliche Schulungen und Zertifizierungen weitergebildet, um Ihnen ein Optimum an Fachkompetenz und Betreuung zu vermitteln.

Unsere Kunden

eb-Qual zählt mittel- bis grosse Unternehmen sowie multinationale Unternehmen zu ihren Kunden. Die Zufriedenheit unserer Kunden ist entscheidend und wir bemühen uns, den Erfolg unserer Projekte zu gewährleisten. Unsere bescheidene Grösse ermöglicht eine einfache Anpassung und wir achten darauf, die am besten geeignete Lösung für die Bedürfnisse unserer Kunden auszuwählen.



Sektor



Grösse

Unsere Lösungen

eb-Qual berät Sie zu den verschiedenen Aspekten der Sicherheit Ihres Unternehmens und zu den besten Lösungen auf dem Markt in den folgenden Bereichen, die wir in drei Hauptkategorien eingeteilt haben: Perimeter & Endpoint, Visibility & Compliance und Network.

Perimeter & Endpoint

DNS Security

Egal wo sich Ihre Anwender gerade aufhalten, die Zscaler Cloud Security Plattform ist immer zwischen ihnen und dem Internet und prüft jedes einzelne Datenbyte. Mit Hilfe von Zscaler lässt sich jede verdächtige oder unbekannte Datei in Echtzeit isolieren, ohne dabei den Datenverkehr per Backhauling in das Datenzentrum transportieren zu müssen. Leiten Sie einfach Ihren Internet-Datenverkehr zu Zscaler – hierzu muss keine Hardware gekauft und keine Software aktualisiert werden.

Email Security & Archiving

E-Mail-Sicherheit ist die Grundlage aller Computersicherheit. Die mit Phishing, Ransomware, Hacking oder einfachen Spam-Angriffen verbundenen Risiken sowie fehlende Archivierung können zum Verlust von Informationen, zum Diebstahl sensibler Daten und zu unerwünschten Kosten führen. Die zentrale E-Mail-Archivierung reduziert den Bedarf an E-Mail-Speicher auf Servern und erfüllt die gesetzlichen Anforderungen. Sie beseitigt auch die Verwendung von PST-Dateien, welche nur schwer zentral zu verwalten sind.

Endpoint & Server Protection

Die jüngste Vergangenheit hat durch Ereignisse wie WannaCry aufgezeigt, dass klassische signaturbasierte AV Lösungen keinen geeigneten Schutz mehr bieten können, um Unternehmen gegenüber neuartiger Malware sowie 0-Day Attacken zu schützen.

Secure Access — Mobility

Die Anforderungen an Mobilität stellen Unternehmen vor grosse Herausforderungen, wenn sie ihren mobilen Mitarbeitern Zugriff auf interne Ressourcen oder die Cloud gewähren und gleichzeitig die üblichen Compliance- und Sicherheitsanforderungen erfüllen müssen.

Web Application Firewall

Die Web Application Firewall (WAF) fügt ein zusätzliches Mass an Sicherheit hinzu, indem sie nicht schadhafte Anfragen an die Web-Anwendung blockiert. Herkömmliche Firewalls können solche Anfragen, welche darauf ausgelegt sind, Daten zu stehlen oder den Betrieb einer Website zu beeinträchtigen, nicht mitigieren.

Web Security Proxy

Angriffe zielen auf den am meisten gefährdeten Punkt in Ihrem Netzwerk ab: den Benutzer. Die Angreifer nutzen Lücken, um Benutzer zu infizieren, wenn sie vertrauenswürdige Websites besuchen. Oftmals wird auch versucht, die Angriffe hinter verschlüsseltem SSL- oder CDN-Verkehr zu verbergen. Der Internetzugang muss für jeden Benutzer sicher sein unabhängig davon, um was für ein Device es sich handelt (Computer, Tablet, Smartphone) und wo es sich befindet.

Visibility & Compliance

Activity Monitoring — Auditing

Überwachung ist eine Tätigkeit, und dies ist umso wichtiger, wenn sie zur Überwachung wünschenswerter Änderungen oder im Gegenteil zur Erkennung einer Anomalie verwendet wird. Diese Überwachung ermöglicht Ihnen auch, die Aktivitäten von Benutzern mit privilegierten Berechtigungen zu überwachen und aufzuzeichnen. Das Audit ist ebenso wichtig, weil es Compliance-Anforderungen (DSGVO, ISO, PCI, SOX, SWIFT, ...) auf einfache, zuverlässige und effiziente Weise erfüllt.

Breach & Attack Simulation

Breach & Attack Simulationen (BAS) sind fortschrittliche Methoden zum Testen Ihrer Computer- und Netzwerksicherheit. Diese Simulationen identifizieren Schwachstellen in Ihren Umgebungen, indem sie mögliche Angriffstechniken auf verschiedenen Angriffspfaden nachahmen und zwar so, wie dies ein Angreifer tun würde. Eine solche Simulation verhält sich wie ein kontinuierlicher und automatisierter Penetrationstest, mit dem Unterschied, dass Sie hierfür keine externen Akteure beiziehen müssen, sondern alles bei Ihnen intern passiert.

Cloud Visibility — CASB

Der Cloud Access Security Broker (CASB) ist eine Lösung und ein Service, der Einblick in die Nutzung von Cloud-Anwendungen, Datenschutz und Governance bietet. Die Lösung ermöglicht es, eine Liste der tatsächlich vom Unternehmen verwendeten Cloud-Dienste zu erzeugen und dabei Sicherheitsregeln wie die Verschlüsselung von Daten in der Cloud anzuwenden. Zusammengefasst bietet das CASB vier Hauptmerkmale: Sichtbarkeit, Datensicherheit, Bedrohungsschutz und Compliance.

Privileged Access Management

Forrester schätzt, dass 80% der Sicherheitsverletzungen privilegierte Anmeldeinformationen beinhalten. Privilegierte Konten sind die größten Sicherheitslücken, denen ein Unternehmen heute gegenübersteht. Privilegierte Konten gibt es überall, in jedem Gerät, jeder Datenbank, jeder Anwendung und jedem Server im Netzwerk wie auch in der Cloud. Privilegierte Konten sind ein Sicherheitsproblem und erfordern einzigartige Steuerelemente, um alle privilegierten Aktivitäten zu schützen, zu überwachen, zu erkennen, zu alarmieren und darauf zu reagieren.

Security Awareness

Die Mitarbeiter Ihres Unternehmens sind eines der ersten Ziele von Cyber-Angriffen und können aufgrund von Unachtsamkeit oder Unkenntnis der Risiken mit nur einem Klick schwerwiegende Schäden anrichten. Machen Sie Ihre Mitarbeiter auf die verschiedenen Angriffe wie Spam, Malware, Phishing usw. aufmerksam. und bringen Sie ihnen bei, wie sie im Zweifelsfall reagieren sollen. Unsere Lösungen ermöglichen es auch, ihre Erfahrungen regelmässig zu testen und so das Risiko besser zu kontrollieren.

SIEM — Log Management

Mit dem Security Information & Event Management (SIEM) können Sicherheitsteams Angriffe in der IT-Infrastruktur durch Ausnutzung, Filterung und Korrelation aller gesammelten Protokolle schnell erkennen. Dies wird das Zentralisierungstool für alle Protokolle (SEM) sein, aber auch die Plattform für Analyse, Compliance und Reporting (SIM). Das SIEM wird die Sicherheitsziele erreichen und dazu dienen, Angriffe zu erkennen, die Einhaltung von Vorschriften zu überwachen und auf Vorfälle zu reagieren. Ihre Protokolle werden archiviert und Reports können schnell erstellt werden.

Network

DDOS Protection

Eine Distributed Denial of Service (DDoS) Attack versucht durch eine gezielt herbeigeführte Überlastung die Nichtverfügbarkeit eines Internetservices (z.B. Weppage) herbeizuführen. Diese DDoS Angriffe sollten in der Regel zweistufig abgefangen werden, erste Stufe beim Netz-Provider für Volumenangriffe und zweite Stufe Vorort um auch gezielte dedizierte Angriffe abzuwehren.

Discovery Automation

Administratoren verlieren oft den Überblick darüber, was sich in ihren Netzwerken für Devices, IP Adressen etc. befinden. Mittels Network Discovery werden alle sichtbaren Geräte inkl. IP- Adresse sowie des entsprechenden Switchports sichtbar gemacht.

DNS — DHCP — IPAM

DDI ist eine Abkürzung für die Integration von DNS, DHCP und IPAM (IP-Adressverwaltung) in einen einheitlichen Dienst oder eine einheitliche Lösung. DDI umfasst die Grundlage von Kernnetzwerkdiensten, die die gesamte Kommunikation über ein IP-basiertes Netzwerk ermöglicht.

Load Balancing — ADC

Load Balancer (SLB) und Application Delivery Controller (ADC) verteilen mittels Lastverteilung grosse Mengen von Anfragen auf mehrere parallel arbeitende Systeme und unterstützen sie im Bereich Application-Networking Funktionen wie Datenbank-Load-Balancing und Lastverteilung auf mehrere Firewalls. Zudem beinhalten sie erweiterte Security-Funktionen und sind als «on-premises» oder auch als Cloudlösung verfügbar.

Services

eb-Qual berät Sie zu den verschiedenen Aspekten der Sicherheit Ihres Unternehmens und empfiehlt Ihnen die besten Marktlösungen in den folgenden Bereichen, die wir in drei grosse Kategorien eingeteilt haben: Perimeter & Endpoint, Visibility & Compliance und Network.

Managed Services

Unsere Dienstleistungen beinhalten auch Managed Services, welche Sie bequem von wiederkehrenden Know-how und arbeitsintensiven IT-Tätigkeiten entlasten und Ihnen Zeit, Kosten und Aufwand sparen. In diesem Zusammenhang bieten wir von Lösungen von Remote-Service bis hin zu ausgewählten Full-Managed-Lösungen an.

Support

- Follow-up bei Wartungsverträgen
- Hilfe bei der Fehleranalyse und -behebung
- Hilfe bei dem Ticketmanagement
- Hilfe bei der Behebung von Hardware und Softwareproblemen

24x7 on Call Services

Bei Anfragen bieten wir auch einen 24x7 On-Call Service.

Ausgewählte Audits

Wir bieten Audits für ausgewählte Systemumgebungen von CyberArk, Infoblox, BlackBerry, PulseSecure und Cisco AMP E-Mail Security Lösungen an. Egal, wo Sie diese Lösungen erworben haben, wir beginnen mit einer grundlegenden Analyse Ihrer Systemeinstellungen, der Integration in die gesamte ICT-Umgebung und Konformität mit den Standards (z. B. Patches und Hardening auf Servern, Rollensegmentierung, Richtlinieneinstellungen, Verfügbarkeitssicherung und Notfallwiederherstellung). Die Verwendung und Dokumentation der zugehörigen ICT- und Organisationsprozesse sowie die spezifische Risikobewertung werden bereitgestellt.

Consulting

Während der Sicherheitsbeurteilung erhalten Sie von eb-Qual einen vollständigen Bericht über die aktuelle technische Situation und die Risiken sowie unsere detaillierten Empfehlungen. Egal, ob Sie eine Sicherheitsberatung oder eine Gesamtbewertung Ihrer ICT-Infrastruktur wünschen, eb-Qual ist Ihr Partner.

Nach dieser Bewertung können wir Sie sowohl auf technologischer als auch auf organisatorischer Ebene unterstützen. Unser Know-how geht vom Strategischen über das Konzeptionelle bis hin zum konkreten Umsetzen und Implementieren.

Installation & Maintenance

Wir sorgen für die Installation, Konfiguration und Wartung Ihrer Geräte mit Professionalität und Effizienz.

Solution Design

- Architektur der Lösung
- Proof of Concept
- Projektmanagement

Route André Piller 33 A | 1762 Givisiez | T +41 26 407 70 80 | info@eb-qual.ch
Oberfeldstrasse 20 | 8302 Kloten | T +41 43 211 47 20 | info@eb-qual.ch