



DAS MACHT BRIVO CYBERSICHER

Cybersicherheit ist ein zentraler Bestandteil unserer Arbeit. Wir wenden drei bewährte Verfahren an, um eine Plattform mit integrierter physischer Sicherheit und Cybersicherheit bereitzustellen und so dem Vertrauen unserer Kunden Rechnung zu tragen.



SO ENTWERFEN WIR PRODUKTE

Entwickelt mit verschlüsselter Gerätekommunikation:
256-Bit-Verschlüsselung¹

Minimieren Sie Ihr Gefahrenpotenzial für Cyber-Angriffe:
Keine offenen Inbound-Ports, die böswillige Angriffe begünstigen²

Überwachung von Bot- und DDoS-Angriffen:
Echtzeit-Warnungen, um Gegenmaßnahmen zu ergreifen³

SO SETZEN WIR ANWENDUNGEN EIN

Regelmäßige und automatische Software-Updates:
Sie sind vor den neuesten Cyber-Bedrohungen geschützt

Dreifache Redundanz:
Gewährleistet hohe Verfügbarkeit⁴



SO FÜHREN WIR UNSER UNTERNEHMEN

Ausführliche interne Schulung:
Technische und sicherheitsrelevante Schulungen für unsere Entwickler, Testingenieure und sonstigen Mitarbeiter

Jährliche Audits durch externe Prüfer:
Bestätigt durch mehr als ein Jahrzehnt an Informationssicherheitsaudits⁵

ZERTIFIZIERUNGEN



GLOSSAR

1. Zum Schutz des Daten- und des Kontozugriffs unterstützen der ACS6000 und der ACS300 den neuesten Standard und längere Schlüssellängen: TLS1.2+ mit AES-256-Verschlüsselung (dieselbe Sicherheitsstufe, der Banken vertrauen) und ein SHA256-Zertifikat mit einem 4096-Bit-Schlüssel.
2. Brivo-Kontrollpanels kommunizieren ausgehend nur auf Port 443. Eliminierung von "Angriffsvektoren", die durch offene Ports in Ihrem Netzwerk entstehen.
3. Komponenten, die sowohl böswillige "Bots" als auch DDoS-Attacken erkennen, sind in unseren 'Brivo Access'-Cloud-Service eingebettet.
4. Jede Produktionskomponente von Brivo Access hat ein redundantes Gegenstück; einschließlich Firewalls, Load Balancer, Webserver, Anwendungsserver und Datenbankserver.
5. Brivo setzt angemessene administrative Kontrollen ein, um vertrauliche Informationen zu schützen. Wir setzen die Kontrollen auf überprüfbar und messbar Weise um. Unabhängige Prüfer kontrollieren zur Verifizierung der Konformität regelmäßig die Bedienelemente und Systeme. Die jährlichen SOC-2-Audits von Brivo werden von einem unabhängigen Service-Auditor durchgeführt.



Copyright 2021 Brivo Systems LLC oder ihre Tochtergesellschaften. Alle Rechte vorbehalten. Brivo und die Brivo-Logos sind eingetragene Markenzeichen oder Markenzeichen der Brivo Systems LLC oder ihrer Tochtergesellschaften in den USA und anderen Ländern. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.