Diligent

10 FRAGEN

zur Beurteilung der Sicherheit von Board-Portalen

Unternehmen, die sich an einen Board-Portal-Anbieter wenden, vertrauen diesem die Sicherheit ihrer sensiblen Dokumente an. Außerdem erwarten Sie ein System zur Zugriffsverwaltung. Bei diesem Vertrauen geht es um weit mehr als nur um Technik. Führungsgremien, administratives Personal, Justitiare und CIOs müssen sich vollkommen auf die Sicherheit verlassen können, die der Board-Portal-Anbieter verspricht.

Im Folgenden finden Sie 10 Fragen, die sich jedes Unternehmen bezüglich möglicher Board-Portal-Anbieter stellen sollte:

1 Investiert der Anbieter ausreichend in Forschung und Entwicklung im Bereich Cybersecurity?

Ständig entstehen neue Bedrohungen. Nicht nur die Technologie, auch die Hackerszene entwickelt sich weiter. Das Bild des einsamen Hackers ist überholt. Heute sind es ganze Organisationen, von denen die Bedrohung ausgeht. Sie sind in der Lage, Ausfälle von globalem Ausmaß zu verursachen. Board-Portal-Anbieter sollten Forschungs- und Entwicklungskapazitäten nachweisen können, um neuen Bedrohungen wirksam begegnen zu können.

2 Wie hält es der Anbieter mit der Transparenz seiner Sicherheitsverfahren?

Der Anbieter sollte in der Lage sein, die bestehenden physischen Sicherheitsmaßnahmen (den Schutz von Servern, Routern und weiteren Geräten), Screeningverfahren bei der Neueinstellung, interne Kontrollen, Systemüberwachung (zur Identifikation von Angriffen) und sicherheitsrelevante Zwischenfälle in der Vergangenheit sowie Abhilfemaßnahmen genau zu erläutern.

3 Erfüllt der Anbieter die höchsten Branchenstandards?

Board-Portale müssen als Drittanbieter-Lösungen, die vertrauliche Informationen enthalten, die Sicherheitsstandards der anspruchsvollsten IT-Bereiche einer Reihe von Branchen erfüllen. Unerlässlich hierbei sind: jährliche Audits nach SOC/SSAE 16 ohne Beanstandungen (Berichtsverfahren der Anbieter hinsichtlich interner Kontrollen), ISO 27001-Sicherheitszertifizierung (Konformität der Informationsmanagement-Sicherheitssysteme des tatsächlichen Softwareanbieters mit internationalen Normen (im Gegensatz zur Konformität des Rechenzentrums)).

4 Lässt der Anbieter Penetrationstests durch Dritte zu?

Die meisten Board-Portal-Anbieter führen im Rahmen von Qualitätskontrollen Penetrationstests durch. Portale mit hohen Sicherheitsstandards führen diese Tests nicht nur jährlich, sondern praktisch fortlaufend durch, um mit der Bedrohungsentwicklung Schritt zu halten. Darüber hinaus sollten Kunden und potenzielle Kunden eigene Sicherheits- und Penetrationstests durchführen (oder Drittanbieter mit diesen beauftragen) dürfen. Dies stärkt nicht nur in hohem Maße das Vertrauen, sondern ist auch ein deutliches Bekenntnis dazu, dass es sich bei Sicherheit letztendlich um ein gemeinsames Anliegen handelt.

5 Nutzt der Anbieter Plattformen oder Software von Drittanbietern?

Viele Board-Portale beruhen auf kommerziellen Plattformen oder verlassen sich in bestimmten Bereichen der Software auf vorgefertigte Plug-Ins. Diese Drittanbieter-Elemente weisen jeweils eigene Sicherheitslücken auf, die für Hacker gerade aufgrund der weiten Verbreitung dieser Plattformen und Plug-Ins von Interesse sind, und wurden nicht speziell für die Anforderungen von Board-Portalen konzipiert. Board-Portale sollten mit Sicherheitsmerkmalen ausgestattet sein, die von Grund auf in die Anwendungen integriert wurden.

6 Welche physischen Sicherheitsmaßnahmen bietet der Anbieter?

Digitale Daten gelten allgemein als immateriell. Dabei gerät in Vergessenheit, dass diese Daten auf allzu materiellen Servern gespeichert werden. Diese Rechenzentren benötigen Schutz durch Wachpersonal vor Ort, Überwachungskameras und vielschichtige Zutrittssicherungen. Die Server selbst sollten sich in Sicherheitsgehäusen befinden. Die Daten einzelner Unternehmen müssen physisch voneinander getrennt gespeichert werden. Kryptographische Schlüssel müssen in gepanzerten und manipulationssicheren Safes aufbewahrt werden.

AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE | Laden im App Store | Downloaden im Windows Store

Diligent ist eine Marke der Diligent Corporation, registriert in den USA. Marken von Dritten sind Eigentum der jeweiligen Inhaber. ©2015 Diligent Corporation. Alle Rechte vorbehalten.

7 Wie hoch ist der Grad an Datenredundanz?

Werden Backups erstellt? Übernehmen bei Ausfällen Recovery-Systeme die Aufgaben der primären Rechenzentren? Board-Portal-Anbieter müssen geografisch weit voneinander entfernt liegende Rechenzentren nutzen, damit ausgeschlossen ist, dass ein Katastrophenfall, der zum Ausfall eines Standortes führt, auch den Sekundärstandort betrifft. Die Redundanz muss zusätzlich durch durchgängige Echtzeitüberwachung der Datenleistung gewährleistet werden

8 Lässt sich der Portal-Zugriff auf ein bestimmtes Gerät beschränken?

Mitglieder von Führungsgremien kommen aus den verschiedensten Ländern und sind häufig auf Reisen. Der Sicherheit von Mobilgeräten kommt daher oberste Priorität zu. Lässt sich der Zugriff auf ein bestimmtes, beim Portal registriertes Gerät einschränken? Besteht die Möglichkeit, den Zugriff über Browser zu unterbinden? Mit Lösungen zur Geräteautorisierung können Unternehmen den Zugriff über unbekannte, nicht vertrauenswürdige Geräte unterbinden. Daraus ergibt sich eine bessere Kontrolle von Zugriffsrechten und der Standorte.

9 Gestattet der Anbieter, das Sicherheitsniveau des Portals selbst zu konfigurieren?

Jede Lösung besteht aus einem Kompromiss zwischen Benutzerfreundlichkeit und Sicherheit. Deshalb suchen unterschiedliche Unternehmen unterschiedliche Lösungen. Die Funktionen eines Board-Portals sollten sich an die jeweiligen Sicherheitsanforderungen eines Unternehmens anpassen lassen (z. B. unterschiedlich starke Kennwörter zulassen, Sperrrichtlinien bieten sowie Optionen zum Exportieren und Drucken von Sitzungsunterlagen festlegen).

10 Ist zusätzlich zu den Sicherheitsfunktionen des Portals Kundensupport vorhanden?

Ganz gleich wie sicher ein Portal auch sein mag, damit zeitnah Maßnahmen ergriffen werden können, ist eine Überwachung durch Personal unverzichtbar. Gibt beispielsweise ein Vorstandsmitglied das Kennwort mehrmals hintereinander falsch ein, sollte sofort ein Anruf des Supports erfolgen, um Hilfe anzubieten und den Grund für die wiederholten erfolglosen Versuche zu ermitteln.

Für weitere Informationen oder um eine Demo anzufordern, kontaktieren Sie:

E-Mail: **info@diligent.com**

Telefon: **0800 7237849**

Website: **www.diligent.com**

C0083_DE