Cybersecurity und der Rollenwandel in den Führungsgremien: **Von der Aufsicht zum Vorbild**

Jeffry Powell
Executive Vice President, Amerika

Charlie Horrell
Geschäftsführer EMEA

Al Percival
Geschäftsführer Australien und Neuseeland

Brian Locke
Sicherheitsdirektor

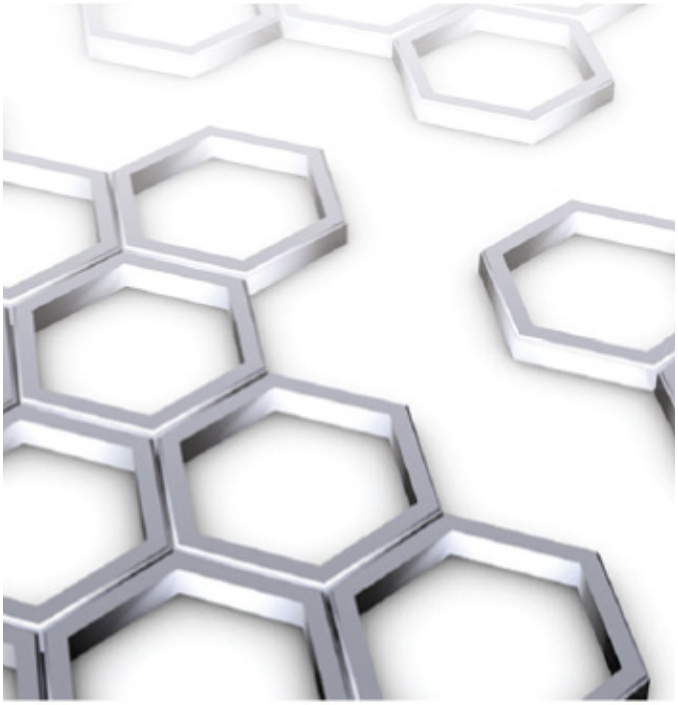
Bei einem Diebstahl von Kundendaten rollen heute in den Führungsetagen nicht selten auch Köpfe. Daher wird die Aufsicht der Cybersecurity immer mehr zur Aufgabe des Aufsichtsrats und der Unternehmensführung. Mit Blick auf ihre eigenen Sicherheitsvorkehrungen im Internet dagegen ist man bei den Führungsgremien oft weniger kritisch. Dieser Artikel stellt einen Bewertungsrahmen für Führungsgremien vor und setzt dabei den Fokus auf drei wesentliche Faktoren: den Speicherort der Daten, die Stärke des Datenschutzes und die Zugriffskontrolle.

Die aktive Einbindung der Unternehmensspitze in das Thema Cybersecurity wird nicht nur von interner Stelle verlangt. Auch Regulierungsbehörden stellen mittlerweile höhere Erwartungen. Die US-Börsenaufsichtsbehörde SEC zum Beispiel weist auf die Bedeutung des Einbezugs von Cybersecurity-Prozessen und -Vorfällen bei der Veröffentlichung von Risikofaktoren und wichtigen Ereignissen eines börsennotierten Unternehmens hin[1]. Und wenngleich diese Regelungen nicht für Privatunternehmen und gemeinnützige Organisationen gelten mögen, fordern deren Inhaber, Geschäftspartner und Geldgeber ebenso die Einhaltung strenger Standards.

Obwohl das Führungsgremium für die Beaufsichtigung der Cybersecurity zuständig ist, wird oftmals ein kritisches Glied in der Sicherheitskette vernachlässigt: die eigene Rolle des Führungsgremiums als Verwahrer sensibler Informationen über das Unternehmen. Schließlich werden von Führungsgremien regelmäßig vertrauliche Finanz- und Vertriebsdaten sowie geheime Strategiepläne, Richtlinien zur Vergütung von Mitgliedern der Geschäftsleitung und andere privilegierte Informationen bearbeitet, gespeichert und intern weitergegeben. Der unbefugte Zugriff auf jede dieser Informationen könnte schwere Konsequenzen nach sich ziehen.

Das Problem ist, dass das Führungsgremium durch seine übergeordnete Stellung gegenüber dem Unternehmen häufig nicht in die unternehmenseigenen Prozesse mit einbezogen wird. Wenn sich der CIO oder der Datenschutzbeauftragte mit der Cybersecurity des Unternehmens befasst, lässt

Diligent



er die Sicherheit des Führungsgremiums häufig außen vor, da sie möglicherweise nicht in seine Zuständigkeit fällt, sondern in die des Unternehmenssekretariats oder der Rechtsabteilung.

Zudem lässt sich nicht leugnen, dass bei den verschiedenen möglichen Maßnahmen im Bereich Cybersecurity stets zwischen Bequemlichkeit und Effektivität abgewogen werden muss. Aufgrund der gehobenen Position von Mitgliedern des Führungsgremiums und der Geschäftsleitung herrscht eine natürliche Neigung, jegliche Unannehmlichkeiten für diese Gruppe möglichst gering zu halten.

Die Folge dieser „Einschränkungsfreiheiten“: Die Mitglieder des Führungsgremiums wählen verständlicherweise oft möglichst bequeme Wege, um an ihre Informationen zu kommen, diese zu speichern und weiterzugeben. Leider sind diese meist deutlich unsicherer als die übliche Vorgehensweise des Unternehmens. Dazu zählt das Verschicken von Geschäftsleitungs-, Vorstands- und Aufsichtsratsunterlagen per Post oder das Senden von PDFs als E-Mail-Anhang.

Weitere Zugeständnisse werden häufig bei den Kennwörtern gemacht. Anstatt sichere Kennwörter vorzuschreiben, die keine Wörter des normalen Sprachgebrauchs enthalten und aus unterschiedlichen Zeichenarten bestehen, werden einfache Kennwörter wie der Vorname des eigenen Kindes gestattet. Wenngleich diese Vorgehensweisen oft keine systematische Praxis, sondern das Ergebnis von Ad-hoc-Entscheidungen darstellt, werden sie nur selten infrage gestellt.

Angesichts der erhöhten Bedrohungslage wird von Führungsgremien und der Geschäftsleitung mehr verlangt als nur die Beaufsichtigung der Cybersecurity eines Unternehmens. Vielmehr müssen sie mit gutem Beispiel vorangehen und von oberster Stelle ein Zeichen für sorgsamen Umgang mit den Sicherheitsprozessen setzen.

EIN RAHMEN ZUR BEWERTUNG DER SICHERHEIT VON FÜHRUNGSGREMIEN

Führungskräfte, die Orientierungshilfen für die Bewertung der Internet-Sicherheit ihres Unternehmens suchen, sehen sich häufig mit einem Gewirr unverständlichen Fachjargons konfrontiert. Glücklicherweise lässt sich anhand der folgenden drei einfachen Fragen mehr Klarheit verschaffen:

1. Wie werden die Informationen des Führungsgremiums gespeichert?

2. Wie gut sind die Daten geschützt?

3. Wer kontrolliert den Zugriff?

Diese drei Fragen können dabei helfen, die aktuellen Praktiken des Führungsgremiums in Bezug auf die Sicherheit des Informationsaustauschs, der Kommunikation und der Zusammenarbeit zu evaluieren und kann als Basis zur Bewertung alternativer Lösungen genutzt werden.

Wie werden die Informationen des Führungsgremiums gespeichert?

Bei jeder Sicherheitsbeurteilung sollte zunächst geprüft werden, wer für die Daten verantwortlich ist. Wenn nicht bekannt ist, wer die Verantwortung trägt, wo sich die Informationen befinden und nicht kontrolliert werden kann, wohin sie gelangen können, steht dies für eine höchst unsichere Lösung.

Aus diesem Grund ist auch der Versand von Sitzungsunterlagen per E-Mail in Form von PDF-Dateien nicht sicher. Dateien können versehentlich an falsche Adressaten versandt oder weitergeleitet werden oder in privaten E-Mail-Konten mit minimaler Sicherheit aufbewahrt werden. Dasselbe gilt für offene Plattformen zum Datenaustausch, bei denen Daten „in der Cloud“ gespeichert werden. Das heißt praktisch, dass sich Ihre Dateien auf irgendeinem beliebigen Server im Cloud-Netzwerk befinden können. Als Nutzer können Sie nie wissen, wo genau sie gespeichert sind.

Aufgrund dieser Unklarheit wurde das Konzept überhaupt als „Cloud“ (engl. Wolke) bezeichnet. Ein Grund für die Popularität von Cloud-Datenspeichern bei ihren Nutzern, ist neben den Zugriffsmöglichkeiten von jedem Ort aus, die Annahme, die Systeme seien relativ sicher.

Allerdings zeigen prominente Hacking-Fälle, bei denen beispielsweise Kennwörter und Prominentenfotos von Cloud-Konten veröffentlicht wurden[2], wie falsch diese Annahme ist. Auch wenn bei gehosteten Board-Portalen der Eindruck einer Cloud nahe liegt – und sie oft fälschlicherweise als „Cloud-basierter Speicher“ bezeichnet werden – gibt es dennoch entscheidende Unterschiede.

So wird zum Beispiel bei Board-Portalen eindeutig geregelt, wo Ihre Daten auf dem gehosteten System gespeichert sind. Außerdem werden die Informationen jedes gehosteten Unternehmens streng voneinander getrennt aufbewahrt. Zu wissen, wo sich Daten befinden und die entsprechenden Sicherheitsmaßnahmen zu kennen, bietet wesentlich bessere Kontrollmöglichkeiten darüber, wer auf die Informationen zugreifen kann und schafft Vertrauen.

Wie gut sind die Daten geschützt?

Ebenso wichtig wie eine strenge Kontrolle über den Verbleib der Daten sind die Berechtigungsprofile, so dass nur autorisierte Nutzer darauf zugreifen können. Ergänzt wird das durch die Verschlüsselung der Daten. Nur Personen mit entsprechenden Zugriffsrechten können die Aneinanderreihung scheinbar bedeutungsloser Nullen und Einsen wieder in sinnvolle Daten entschlüsseln. Gedruckte Sitzungsunterlagen sind natürlich in keiner Weise verschlüsselt, d. h. die Informationen können ganz einfach von jedem gelesen und kopiert werden, dem sie in die Hände fallen.

Und es mag zwar stimmen, dass per E-Mail gesendete oder in der Cloud gespeicherte PDFs verschlüsselt und durch Kennwörter geschützt werden können. Allerdings sind dann diejenigen, die das Material verteilen und diejenigen die sie empfangen, jeweils für ihre Kennwörter verantwortlich. Außerdem sind auf diese Weise „geschützte“ Dokumente weiterhin anfällig für Brute-Force-Angriffe durch entsprechende, leicht zugängliche Software, mit der gängige Passwörter automatisiert durchprobiert werden. Gehostete Board-Portale verwenden üblicherweise eine 256-Bit-Verschlüsselung. Da ein solches System mehr Kombinationsmöglichkeiten als Sterne im Universum beinhaltet, lässt sich mit ziemlich hoher Sicherheit sagen, dass selbst der ausdauerndste Hacker mit der fortschrittlichsten Technologie eine halbe Ewigkeit brauchen würde, um den Code zu knacken.

Wer kontrolliert den Zugriff?

Egal wie stark ein Verschlüsselungssystem auch sein mag, jeder der über den richtigen Schlüssel verfügt, kann auf die Informationen zugreifen. So ist jeder, der das Kennwort für eine geschützte PDF kennt, praktisch der Eigentümer des Dokuments. Gestohlene Kennwörter sind somit gleichzusetzen mit gestohlenen Dokumenten. Doch bei einem gehosteten Board-Portal ist das Kennwort nicht alles. Man kann zwar damit auf das Portal zugreifen, aber weil die Verschlüsselungscodes zum Schutz der Geschäftsleitungs-, Vorstands- und Aufsichtsratsunterlagen über das System kontrolliert werden, sieht die angemeldete Person nur, was sie sehen darf. Ein gutes Portal darf niemals die Kontrolle über die Dokumente verlieren. Die Folgen für die Sicherheit wären beträchtlich.

Angesichts der erhöhten Bedrohungslage wird von Führungsgremien und der Geschäftsleitung mehr verlangt als nur die Beaufsichtigung der Cybersecurity eines Unternehmens. Vielmehr müssen sie mit gutem Beispiel vorangehen und von oberster Stelle ein Zeichen für sorgsamen Umgang mit der Sicherheitsprozessen setzen.

Wenn ein Board-Portal-Kennwort gestohlen wird, kann der Administrator den Zugriff für dieses Kennwort einfach sperren. Und sobald vertrauliche Dokumente nicht mehr benötigt werden, kann der Administrator eine „virtuelle Reinigung“ durchführen, bei der die Dokumente für jeden, der versucht, mit einem gestohlenen Kennwort auf das Benutzerkonto zuzugreifen, verschwinden. Neben der Zugangsbeschränkung per Kennwort, kann der Portaladministrator den Zugriff auf bestimmte Dokumente gemäß Kriterien wie etwa der Mitgliedschaft in einem Ausschuss einschränken. So sind diese Dokumente beispielsweise nur für Mitglieder des Prüfungs- oder Vergütungsausschusses sichtbar. Der Administrator kann außerdem kontrollieren, mit welchem Gerät ein Nutzer auf das System zugreifen kann.

1. „CF Disclosure Guidance Topic No. 2: Cybersecurity“, Abteilung der US-Börsenaufsichtsbehörde SEC. Wall Street Journal, „Apple Denies iCloud Breach: Tech Giant Says Celebrity Accounts Compromised by ‘Very Targeted Attack’“

2. September 2014. **http://online.wsj.com/articles/apple-celebrityaccounts-compromised-by-very-targeted-attack-1409683803**

DIE UNTERNEHMENSLEITUNG MUSS EIN SIGNAL SETZEN

Das Thema Cybersecurity mag zwar in immer mehr Unternehmen einen festen Platz auf der Tagesordnung von Führungsgremien und Geschäftsleitungen haben, aber das allein ist nicht genug. Die Unternehmensleitung muss das Sicherheitsbewusstsein täglich vorleben.

Mit der richtigen Plattform für den Umgang mit Sitzungsunterlagen des Führungsgremiums kann sichergestellt werden, dass wichtige Sicherheitsmaßnahmen in der Führungsetage eingehalten werden. Außerdem wird so die richtige Botschaft ausgesandt: Cybersecurity geht alle an.

Diligent

Entfalten Sie das volle Potenzial: Sichere Informationen für Top-Entscheider

Mithilfe von Diligent nutzen weltweit führende Unternehmen das volle Potenzial – sicherer – digitaler Zusammenarbeit, indem sie ihren Führungsgremien und Managementteams die Werkzeuge an die Hand geben, die eine schnellere und leichtere Entscheidungsfindung ermöglichen. Über 3.100 Kunden in mehr als 50 Ländern vertrauen auf Diligent für den unmittelbaren Zugriff auf ihre zeitkritischen und vertraulichen Informationen für ihre Entscheidungsträger sowie zu den für die Erstellung, Verteilung und Durchsicht erforderlichen Tools. Die Lösung Diligent Boards (vormals Diligent Boardbooks) beschleunigt und vereinfacht, wie Geschäftsleitungs-, Vorstands- und Aufsichtsratsunterlagen erstellt und über iPads, Windows-Tablets, PC's und Browser bereitgestellt werden. Sie bietet auch ganz handfeste Nutzenvorteile, wie niedrigere Erstellungskosten und Zeiteinsparungen für die Administration und die IT und sie hilft Nachhaltigkeitsziele zu erfüllen.

Besuchen Sie uns auf www.diligent.com und finden Sie uns unter DIL auf der neuseeländischen Börse (NZX).

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