

Markus Seyfried^{*)}

Informationssicherheit im Aufsichtsrat durch elektronische Datenräume

Bei allen Kommunikationsvorgängen im Aufsichtsrat geht es durchweg um vertrauliche, unternehmenskritische Daten. Ihr Verlust durch Spionage oder falsche Nutzung hat meist negative Folgen für das Unternehmen. Ein aktives Risikomanagement muss deshalb geeignete Maßnahmen zum Schutz vertraulicher Daten bereitstellen. Elektronische Datenräume gelten inzwischen als Königsweg zur Umsetzung einer durchgängigen Sicherheitsstrategie in der AG. Zum ersten Mal werden sämtliche Sicherheitsmechanismen, die technisch verfügbar sind, unter einer übersichtlichen Oberfläche zusammengeführt. Und sie gestatten neben dem sicheren Zugang für die Aufsichtsratsmitglieder auch die Einbindung externer Teilnehmer wie Wirtschaftsprüfern oder Investmentbanken.

„Elektronische Datenräume schützen vor dem Verlust vertraulicher Daten.“

I. Gefahrenpotenziale

Das Jahr 2007 gilt unter Sicherheitsexperten als Wendepunkt in Bezug auf die Bedrohungsszenarien im elektronischen Datenverkehr. Erstens hat die Zahl der Angriffe dramatisch zugenommen. So wurde allein von Januar bis Oktober 2007 eine Zunahme von Malware wie Viren, Trojanern oder Botkits um das Sechzehnfache registriert. Damit einher ging zweitens eine enorm gestiegene Qualität der Bedrohungs-Software. Beide Entwicklungen haben unmittelbar mit der Professionalisierung der Malware-Szene zu tun.

Zu den profitabelsten Formen von Online-Kriminalität zählen der Diebstahl von unternehmenskritischen Daten durch das technische Anzapfen von Informationsflüssen, das unbefugte Abfragen von kritischen Informationen über Phishing und nicht zuletzt das gezielte Ausspähen von Identitäten zum Zweck der Cyber-Erpressung. Mit den so gewonnenen Daten kann beispielsweise ein Mitarbeiter einer AG dazu veranlasst werden, vertrauliche Dokumente von dem Fileserver, auf dem sie gespeichert sind, zu kopieren.

Oft ist es aber gar nicht ein gezielter elektronischer Angriff, der vertrauliche, hochsensible Daten in unbefugte Hände kommen lässt. Noch immer ist menschliches (Fehl-)Verhalten die größte „Gefahrenquelle“. Im gerade beschriebenen kriminellen Kontext kann sich der Angreifer beispielsweise auch durch Bestechung in den Besitz der Daten bringen. Manchmal genügt jedoch schon die Eingabe einer falschen E-Mail-Adresse. Wenn dann die aktuellen Quartalszahlen als Anlage versendet werden, können sie in falsche Hände gelangen. Oder noch profa-

ner: Ein Aufsichtsratsmitglied vergisst nach der Sitzung, die gedruckten Unterlagen im Schredder zu vernichten und lässt sie im Konferenzzimmer liegen.

Da es bei der Vielzahl der elektronischen Daten und deren internen und externen Distributionswegen in einer AG praktisch unmöglich ist, den durchgängigen Schutz vor Verlust oder Missbrauch im operativen Geschäft zu garantieren, liegt es nahe, für die besonders sensible Kommunikation innerhalb des Aufsichtsrats einen eigenen, besonders gesicherten Bereich zu schaffen – und das ohne Einschränkungen in Bezug auf Funktionalität und Aktualität.

II. Zentraler Datenschutz

Ein aktives Risikomanagement muss prophylaktisch alle im Aufsichtsrat erfolgenden Kommunikationsvorgänge konsequent und wirkungsvoll schützen. Das kann nur in einem exklusiven, geschützten Datenraum, dem Secure Boardroom, erfolgen.

Zentraler, geschützter Datenraum: In dem elektronischen Datenraum werden alle für den Aufsichtsrat relevanten Dokumente in einen zentralen elektronischen Datenpool eingespeist und dort allen Berechtigten zur Verfügung gestellt. Dieser Datenpool befindet sich auf einem gesonderten, besonders gesicherten Rechner, dem so genannten Host oder Server. Er ist physisch und systematisch völlig unabhängig von den operativen IT-Systemen eines Unternehmens und wird von einem externen Dienstleister zur Verfügung gestellt. Die Verwaltung der Daten, d.h. die Zugangsberechtigungen und -kontrollen, Protokollierung aller Arbeitsschritte, Veränderungen und

^{*)} Markus Seyfried, Technikvorstand der Brainloop AG, München.

Ergänzungen sowie sämtliche Sicherheitsfunktionen, übernimmt eine spezielle Software auf dem Server, die ebenfalls extern gestellt wird.

Der Zugriff auf die Daten erfolgt über das Internet mit einem gängigen Internet-Browser. Zusätzliche Softwareinstallationen sind nicht erforderlich. Da ein elektronischer Datenraum für alle Berechtigten gleichzeitig verfügbar ist, können die Dokumente parallel und unabhängig voneinander gesichtet, geprüft, kontrolliert und sogar bearbeitet werden. Diese Funktion wird durch ein integriertes Dokumenten-Management-System gewährleistet. Der Datenraum, und damit die dort eingestellten Dokumente und Dateien, sind mehrfach geschützt.

Authentisierung: Zugang zu diesem Datenraum dürfen ausschließlich befugte Personen erhalten. Eine strenge Berechtigungsprüfung bei der Eingangskontrolle ist unerlässlich – ein einfaches Passwort reicht dazu nicht mehr aus. Zusätzliche Sicherheit verspricht die so genannte 2-Faktor-Authentisierung über Komponenten wie Chipkarte, Fingerabdruckererkennung oder andere biometrische Verfahren. Als praktikabelste Lösung hat sich die Absicherung des Zugangs über das Mobiltelefon des Teilnehmers durchgesetzt. Die hohe Sicherheit dieses Authentisierungs-Verfahrens basiert auf der Nutzung von kurzlebigen Einmalschlüsseln, die per SMS verschickt werden. Da diese Option für jeden Datenraum separat aktiviert werden kann, ist sie auch für den unternehmensübergreifenden Einsatz geeignet.

Verschlüsselung: Sie dient dem Schutz der Daten vor unbefugtem Zugriff in jeder Phase. Merkmal einer echten End-to-End Security-Architektur ist die Verschlüsselung sämtlicher Dokumente auf dem Server, die Verschlüsselung der Dokumente bei der Übertragung und die Verschlüsselung der Dokumente während der Bearbeitung. Durch den Verschlüsselungsschutz der Daten in der zentralen Ablage ist ein Zugriff durch das Betreiberpersonal oder unbefugte Personen zwar möglich, aber unkritisch. Dies gilt auch für den Fall einer unsachgemäßen Entsorgung von Hardwarekomponenten wie Festplatten: Die Daten können zwar ausgelesen, aber nicht genutzt werden. Auch jede E-Mail, jede gesendete Datei, jedes Attachment wird beim Sender verschlüsselt und anschließend beim Empfänger wieder entschlüsselt. Selbst wenn ein elektronischer Übertragungsweg angezapft wird, kann so der Angreifer mit den gestohlenen Daten nichts anfangen, weil sie unleserlich sind.

Papiermanagement: Außerhalb des elektronischen Datenraums ist der Ausdruck von streng vertraulichen Dokumenten untersagt und deshalb erst gar nicht möglich. Ausdrücke innerhalb des elektronischen Datenraums hingegen werden penibel protokolliert und persönlich zugeordnet. Alle Dokumente sind zudem mit einem Wasserzeichen versehen, das personalisiert werden kann, und sie müssen alle spätestens zum Ende der Aufsichtsratssitzung im Schredder vernichtet werden.

Client Security: Die Vertraulichkeit der Daten muss jederzeit und überall gewährleistet sein; und dieser Schutz ist mehrfach sicherzustellen. Einerseits für die Mitglieder des Aufsichtsrats während der Aufsichtsratssitzung und außerhalb der Sitzungen und andererseits zusätzlich für alle externen Teilnehmer.

Dieser Schutz muss auch bei der Präsentation von Dokumenten gewahrt bleiben und ebenso dann, wenn sie alleine oder gemeinsam bearbeitet werden.

So erfolgt die Anzeige von Dokumenteninhalten generell über einen so genannten Secure Document Viewer. Er besitzt eine integrierte Funktion, die die Darstellung in gekachelten Teilbildern anbietet. Durch diese Zerstückelung wird die Weitergabe von Daten erschwert, wenn nicht gar unmöglich gemacht. Denn der Aufwand, der getrieben werden muss, um ein Dokument komplett zu kopieren, wird um ein Mehrfaches gesteigert. Und mit Teilinformationen kann ein Außenstehender wenig anfangen. Zusätzlich werden die Dokumente mit einem Wasserzeichen versehen. Damit ist selbst die Option, die Daten – wie in alten Spionagethrillern – abzufotografieren, verwehrt. Denn einerseits sind die Daten schlechter lesbar, und andererseits ist ihr Ursprung jederzeit nachvollziehbar. So können die Daten präsentiert und editiert werden, ohne die Sicherheit zu beeinträchtigen.

Den Schutz der Dokumente außerhalb der Aufsichtsratssitzungen am Arbeitsplatz übernimmt ein so genannter RMS Connector. Dabei können sie am lokalen Arbeitsplatz oder über einen mobilen Zugang bearbeitet werden. Er regelt die Zugriffsrechte für jeden Benutzer, also ob er lesen, drucken, bearbeiten und/oder weiterleiten darf. Die Rechtevergabe und -kontrolle wird über die Windows Rights Management Services vorgenommen. Da sie ab der Version 2003 in dem Programmpaket Microsoft Office standardmäßig enthalten sind, erfordert dies keine zusätzlichen Softwareinstallationen auf dem PC oder Notebook. Die für die Zugriffskontrolle benötigten Zertifikate und Credentials werden automatisch von dem Server – also dem zentralen Ort, an dem sich der elektronische Datenraum befindet, – an den Client – also den Rechner des jeweiligen Benutzers – gesendet.

Transparenz: Ein wichtiges Element ist die Transparenz sämtlicher Vorgänge und Änderungen bei der Bearbeitung von Dokumenten. Eine Stimme aus der Praxis der Nutzung eines elektronischen Datenraums lautet: „Bei der Konzeption unseres Secure Datarooms wurde besonderer Wert auf den Schutz vor unkontrollierter Verteilung und die lückenlose Nachvollziehbarkeit sämtlicher Änderungen in den Dokumenten gelegt, um so den Corporate Governance-Regularien für die vollständige Dokumentation aller Informationsflüsse Genüge zu tun.“ Die Schaffung eines Datarooms gestattet auch die Einbindung externer Dienstleister und Berater. Je wichtiger und vertraulicher ein Dokument ist, desto größer ist die Wahrscheinlichkeit, dass es häufig mit Wirtschaftsprüfern oder Investmentbanken ausgetauscht und bearbeitet wird. Die Anbindung der externen Beteiligten ist also eine zwingende Anforderung, und auch diese muss völlig transparent erfolgen.

III. Fazit

Der Einsatz eines Secure Boardroom wird als wichtiger Teil des Risikomanagements inzwischen immer mehr zum Standard bei verantwortungsvoll geführten Unternehmen. Damit werden sämtliche Werkzeuge der modernen Informationstechnologie ohne komplexe Softwareintegration flexibel zum Einsatz gebracht.