

Data Turnover Protection

So schützen Sie Ihr Unternehmen vor Datenlecks in der E-Mail-Kommunikation und dem Verlust von Daten bei einem Mitarbeiterwechsel

Mitarbeiter kommen und gehen – Ihre Daten sollten bleiben wo sie sind	1
Kritische Daten müssen im Unternehmen bleiben	2
Auch Produktivitätstools können kontraproduktiv sein	3
Unternehmen müssen flexibel bleiben	4
Schutz vor Datenverlusten	5
Verhindern Sie Datenverluste mit SonicWALL Data Turnover Protection	6
SonicWALL Email Security	7
SonicWALL Continuous Data Protection	8
SonicWALL Network Security	9
SonicWALL Secure Remote Access	10

Mitarbeiter kommen und gehen – Ihre Daten sollten bleiben wo sie sind

Mitarbeiter sind das wertvollste Kapital jeder Organisation. Ihre Arbeit ist von entscheidender Bedeutung für den Erfolg des Unternehmens. Bei einem Personalwechsel müssen geschäftskritische Daten unbedingt im Unternehmen bleiben, damit produktives Weiterarbeiten sichergestellt ist. Mitarbeiterfluktuation gehört zur Tagesordnung, ist aber immer eine Herausforderung – ganz besonders bei der momentanen Wirtschaftslage.

Möchten Sie bei jedem Mitarbeiterwechsel das Risiko eingehen, geistiges Eigentum zu verlieren?



Mitarbeiter, die das Unternehmen verlassen, versäumen es häufig, wichtige Daten, E-Mails und Voicemail-Nachrichten an ihre Nachfolger weiterzuleiten. In manchen Fällen ist kein Nachfolger bestimmt oder die Übergabe ist schlecht organisiert. Egal vor welchem Hintergrund: Mitarbeiterwechsel können die Sicherheit geschäftskritischer Daten und geistigen Eigentums gefährden, die Produktivität beeinträchtigen und dazu führen, dass Geschäftschancen vergeben und Umsätze verloren gehen.

Kritische Daten müssen im Unternehmen bleiben

Wenn Mitarbeiter das Unternehmen verlassen, kann dies die Produktivität beeinträchtigen. Ein reibungsloser Betrieb ist nur gewährleistet, wenn das geistige Eigentum (z. B. Kontaktlisten, Geschäftspläne, Forschungs- und Finanzunterlagen) der Mitarbeiter im Unternehmen verbleibt und nicht in die Hände unberechtigter Dritter gelangt. Damit geschäftskritische Daten und geistiges Eigentum nicht abhanden kommen, brauchen Organisationen automatisierte Regeln, um eventuell verwaiste Daten zu finden und zu schützen.

Bei verwaisten Daten handelt es sich um Geschäftsinformationen, geistiges Eigentum und Anwendungen, die nicht wiederhergestellt werden können, weil die Daten auf Geräten (z. B. Laptops, Smartphones oder PDAs) gespeichert waren, die nicht mehr greifbar sind und für die es kein Backup gibt.



IT-Abteilungen benötigen erschwingliche und gut ausgestattete Backup- und Recovery-Lösungen, mit erkennbar gutem ROI. Gleichzeitig wünschen sich Unternehmen Lösungen, die den Verwaltungsaufwand automatisieren und reduzieren, und so die TCO senken.

Auch Produktivitätstools können kontraproduktiv sein

Es kommt immer wieder vor, dass Mitarbeiter – in Unkenntnis der Unternehmensrichtlinien – sich selbst oder Dritten ohne die Erlaubnis des Unternehmens vertrauliche Dokumente per Mail zusenden – ohne dass es Regelkontrollen gibt, die das verhindern könnten.

Produktivitätstools wie E-Mail können kontraproduktiv sein, wenn damit Geschäftspläne, Finanzunterlagen, Produktentwicklungspläne und andere vertrauliche Dokumente nach außen gesendet werden.



Laut einer kürzlich veröffentlichten Umfrage zum Thema IT-Sicherheit haben 56 % der Angestellten Angst, dass sie entlassen werden und über 50 % der Mitarbeiter haben sich bereits wettbewerbsrelevante Daten ihrer Firma heruntergeladen, um für einen Jobwechsel vorbereitet zu sein. Berichten von ComputerWorld zufolge können Entlassungsgerüchte dazu führen, dass Vertriebsmitarbeiter Unterlagen über Kunden, Bestellungen und Zahlungen an ihre privaten E-Mail-Adressen senden. Und Forrester Research berichtet, dass die häufigste Bedrohung von Mitarbeitern ausgeht, die vor oder kurz nach ihrer Entlassung geistiges Eigentum (strategische Pläne, Kundendaten, etc.) entwenden.

¹ Cyber-Ark Software Inc. 2008 (Bericht vom 2. März 2009 in der Zeitschrift ComputerWorld)

² 2. März 2009.

³ Jonathan Penn, Bericht vom 2. März in der Zeitschrift ComputerWorld.

Unternehmen müssen flexibel bleiben

Angesichts der aktuellen Marktdynamik kann es vorkommen, dass neue Standorte hinzugekauft oder übernommen werden oder dass entlegene Büros eröffnet werden. Auch können Kosteneinsparungen in Form von Umstrukturierungen oder Konsolidierungen nötig werden.

Unternehmen müssen flexibel auf den schnell wechselnden Personalbedarf reagieren können.



Neue oder ehemalige Mitarbeiter, Lieferanten, Berater und Outsourcing-Partner müssen schnell hinzugenommen oder abgezogen werden können.

Data Turnover Protection von SonicWALL: Doppelte Sicherheit für kritische Daten

1 Schließt potentielle Sicherheitslücken beim Versand sensibler Daten über geschäftliche oder private E-Mailkonten.

In Zeiten, in denen Mitarbeiter das Unternehmen verlassen, muss verstärkt kontrolliert werden, dass keine vertraulichen und sensiblen Daten oder geistiges Eigentum (z. B. Geschäftspläne, Forschungs- und Finanzunterlagen, Kontaktlisten, Produktentwicklungspläne, etc.) nach außen gelangen – weder über geschäftliche E-Mail-Konten wie Outlook noch über private Konten wie Gmail®.

Mit Data Turnover Protection lassen sich granulare Regeln für interne, remote tätige und mobile Mitarbeiter, Lieferanten und Berater erstellen und Beschränkungen mit automatisch generierten Antworten durchsetzen – angefangen von freundlichen Erinnerungen bis hin zu blockierten E-Mails.

2 Gewährleistet die Produktivität nach einem Mitarbeiterwechsel durch eine einfache Wiederherstellung wichtiger Informationen.

Unternehmen müssen für die Sicherung und Wiederherstellung aller wichtigen Daten sorgen – auch solcher, die möglicherweise auf Laptops, Smartphones, Heimrechnern oder in Privatordnern vergessen werden, wenn Mitarbeiter das Unternehmen verlassen.

Mit Data Turnover Protection werden Daten, Anwendungen und Einstellungen jedes Mal automatisch gespeichert, wenn sich Mitarbeiter mit dem Netzwerk verbinden, um ihre Geräte auf Servern, Desktop-PCs – und selbst auf mobilen Laptops – zu aktualisieren. Dies geschieht kontinuierlich und nicht nur einmal täglich wie bei der tapebasierten Datensicherung. Das gibt Ihnen die Gewissheit, dass die Daten verfügbar sind, wenn sie gebraucht werden.

Verhindern Sie Datenverluste mit SonicWALL Data Turnover Protection

Jeder Mitarbeiterwechsel bringt Risiken mit sich. Als Antwort auf diese ständige Herausforderung bietet SonicWALL® Data Turnover Protection eine umfassende, abgestimmte Lösung, die vier mehrfach ausgezeichnete SonicWALL-Technologien vereint:

- Email Security
- Backup und Recovery
- Network Security
- Secure Remote Access/SSL VPN

Dank der kombinierten Multi-Layer-Data Turnover Protection-Lösung von SonicWALL können Sie Produktivitätseinbußen durch den Verlust intellektuellen Eigentums nach einem Mitarbeiterwechsel vermeiden.



SonicWALL Email Security

SonicWALL Email Security (SES) ist eine mehrfach ausgezeichnete Anti-Spam-, Anti-Virus-, Anti-Phishing-, Regel- und Compliance Management-Lösung, die High-Performance-E-Mail-Sicherheit bietet. Als Teil von SonicWALL Data Turnover Protection verhindert SonicWALL Email Security dank zuverlässiger, automatisierter Sicherheitsregeln für ein- und ausgehenden Datenverkehr, dass vertrauliche Informationen nach außen dringen. Außerdem prüft die Lösung E-Mails und über 300 Dateianhangformate wie Word, PowerPoint und PDF auf bestimmte Wörter und Formulierungen und reagiert mit adäquaten Maßnahmen.



SonicWALL SES verhindert, dass vertrauliche Informationen und geistiges Eigentum in E-Mail-Nachrichten und -Anhängen nach außen dringen



SES bietet eine benutzerfreundliche webbasierte Verwaltungsoberfläche, mit der sich Verwaltungsregeln für ein- und ausgehende E-Mails einfach implementieren lassen – egal ob sie unternehmensweit oder nur für spezielle Benutzer oder LDAP-Gruppen angewendet werden. Darüber hinaus lässt sich mit SES die Effizienz der Regeln zentral überwachen, da alle betroffenen E-Mails in einen ausgewiesenen Approval-Ordner geleitet werden.

SonicWALL Continuous Data Protection

SonicWALL Continuous Data Protection (CDP) bietet eine durchgängige diskbasierte Datensicherung und -wiederherstellung in einer einzigen, benutzerfreundlichen und zuverlässigen Komplettlösung. Zu den flexiblen Datensicherungsoptionen gehören Offsite-Datenbackup, Site-to-Site-Datenbackup, lokale Archivierung sowie Bare Metal Recovery. CDP sorgt für eine zuverlässige automatisierte Durchsetzung von Backupregeln, die selbst bei reisenden oder remote arbeitenden Laptop-Benutzern greifen, sobald sie sich mit dem Netzwerk verbinden.

SonicWALL CDP schützt vor dem Verlust geschäftskritischer Informationen, wenn Mitarbeiter das Unternehmen verlassen.



Als Teil von SonicWALLs Data Turnover Protection bieten die automatischen diskbasierten Backups von SonicWALL eine kontinuierliche Datensicherung, die jedes Mal ein Backup durchführt, wenn eine Datei aktualisiert wird. So können Sie sich beruhigt zurücklehnen und müssen sich nicht auf tapebasierte Lösungen verlassen, die nur einmal täglich eine Sicherung durchführen und anfällig für Bedienungsfehler sind. Endbenutzer können ganz unkompliziert und ohne die Hilfe der IT-Abteilung ihre Daten in Minutenschnelle wiederherstellen. Auch Administratoren können auf einfache Weise gesamte Workstation- oder Serversysteme mit allen Einstellungen und Anwendungen wie Exchange, SQL Server und Active Directory wiederherstellen.

SonicWALL Network Security

SonicWALL Network Security kombiniert seine patentierte High-Speed Reassembly-Free Deep Packet Inspection™ (RFDPI)-Technologie mit zuverlässigen Unified Threat Management (UTM)-Sicherheitsservices. Als Teil von SonicWALLs Data Turnover Protection verringert Network Security den Datenverlust über Webmail-Services wie Yahoo® oder Gmail. Durch die Aktivierung der Application Firewall-Regeln werden alle ausgehenden E-Mails mit sensiblen oder vertraulichen Informationen erkannt und blockiert. Die Lösung kann außerdem die Übertragung von Dateianhängen in E-Mail-Programmen wie Microsoft® Outlook aufspüren und blockieren.

SonicWALL Network Security beschränkt die unerlaubte Verbreitung von sensiblen und unternehmenseigenen Informationen bei einem Mitarbeiterwechsel.



SonicWALL beschränkt die unerlaubte Übertragung von Dateien durch Einschränken oder Zurücknehmen von FTP-Berechtigungen für bestimmte Benutzer. Auf diese Weise wird die Übertragung spezieller Dateiformate blockiert, die häufig für vertrauliche oder sensible Unternehmensdaten verwendet werden (z. B. Word-, PowerPoint- oder Excel-Dateien). Außerdem lässt sich das File Sharing über Peer-to-Peer-Anwendungen ausschalten.

SonicWALL Secure Remote Access

Als Teil von SonicWALLs Data Turnover Protection bietet SonicWALL Secure Remote Access (SRA) einen sicheren Remote-Zugriff über SSL VPN auf geschäftskritische Ressourcen von nahezu jedem Gerät aus – Desktop-PCs, Laptops, PDAs und Smartphones. Darüber hinaus bietet SonicWALL SRA einen optionalen Remote-Helpdesk-Support für Laptops und PCs, die nicht von der IT-Abteilung verwaltet werden.



SonicWALL SRA bietet eine granulare Zugriffskontrolle und schützt geistiges Eigentum vor unerlaubtem Zugriff über remote oder mobil genutzte Geräte.

Als Teil von SonicWALLs Data Turnover Protection sorgt SonicWALL SRA für eine automatisierte Durchsetzung von Sicherheitsregeln, bei der im Voraus bestimmte Endpunkt-Kriterien abgefragt werden. So müssen Clients beispielsweise über ein gültiges zertifikatsbasiertes Wasserzeichen verfügen. Mithilfe seiner regelbasierten Endpunkt-Kontrolle kann SonicWALL SRA Zugriffsversuche von unverwalteten PC-Terminals in Bürokommunikationszentren, Cafés, Flughäfen oder Hotels erkennen und einschränken. Die Secure Desktop-Funktion von SonicWALL erstellt eine virtuelle verschlüsselte Umgebung, mit der verhindert wird, dass sensible Daten zurückgelassen werden. SonicWALL SRA kann verdächtige E-Mail-Anhänge in Outlook Web Access oder Lotus iNotes blockieren und den Zugriff auf Finanzdaten oder Krankenakten sperren. Mit seiner standardmäßig geschlossenen VPN-Plattform bietet SRA einen „Deny all“-firewallähnlichen Schutz.

Wie erhalte ich weitere Informationen?

Besuchen Sie die Data Turnover Protection-Website.

Klicken Sie hier, um sich unseren SonicWALL-Newsletter zuschicken zu lassen.

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von SonicWALL geben möchten, senden Sie eine E-Mail an folgende Adresse: **feedback@sonicwall.com**.

Weiterempfehlen

Über SonicWALL

Als führender IT-Sicherheitsanbieter sorgt SonicWALL mit seinen intelligenten und dynamischen Service-, Software- und Hardware-Lösungen für den reibungslosen Betrieb von High-Performance-Unternehmensnetzen und senkt nicht nur die Risiken und Kosten, sondern auch die Komplexität. Weitere Informationen erhalten Sie auf unserer Website unter **www.sonicwall.com/de**.