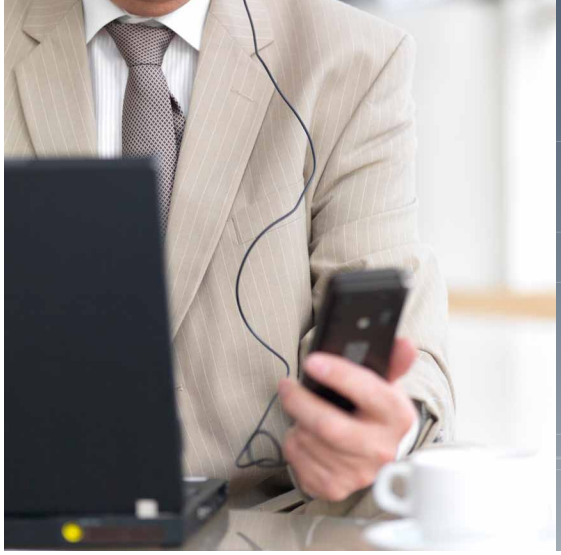
McAfee
An Intel Company

SICHERER ZUGANG ZU SOZIALEN MEDIEN

Lösungsleitfaden

SECURITY CONNECTED-REFERENZARCHITEKTUR

STUFE 1 **2** 3 4 5



80 PROZENT

80 Prozent der Unternehmen setzen LinkedIn als wichtigstes Mittel zum Suchen neuer Mitarbeiter ein.[7]

Security Connected

Das Security Connected-Framework von McAfee ermöglicht die Integration verschiedener Produkte, Services und Partnerschaften zur zentralen, effizienten und effektiven Risikominimierung. Der Security Connected-Ansatz greift auf mehr als zwei Jahrzehnte bewährter Sicherheitspraktiken zurück und unterstützt Unternehmen aller Größen und Bereiche weltweit bei der Verbesserung ihrer Sicherheitslage, Optimierung der Kosteneffizienz von Sicherheitsmaßnahmen sowie der strategischen Anpassung der Sicherheit an Unternehmensinitiativen. Die Referenzarchitektur für Security Connected bietet einen sicheren Pfad von der ursprünglichen Idee bis zur tatsächlichen Implementierung. Durch ihren Einsatz können Sie die Security Connected-Konzepte an Ihre speziellen Risiken sowie an die Infrastruktur und die Geschäftsziele anpassen. McAfee ist stets auf der Suche nach neuen Möglichkeiten, um seine Kunden umfassend zu schützen.

Laut Gartner werden „Social-Networking-Dienste bis zum Jahr 2014 für 20 Prozent der Geschäftsanwender E-Mail als Hauptinstrument für persönliche Kommunikation ersetzen."[1]

Schutz geschäftskritischer sozialer Medien

Herausforderungen

Soziale Medien haben die Welt verändert. Wenn Ihnen diese Aussage hoch gegriffen erscheint, bedenken Sie, wie wir heute Geschäftskontakte, persönliche Beziehungen, Kommunikation, Marketing, Vertrieb sowie zahllose andere Aspekte unseres Geschäfts- und Privatlebens verwalten. Unternehmen stellen immer mehr fest, dass soziale Medien in allen Bereichen nützlich sind: Sie vereinfachen Ihren Mitarbeitern den Kontakt mit Kunden, ermöglichen neue Marketing-Strategien zur Erschließung neuer Einkommensquellen und verbessern die Produktivität. Marketing-Abteilungen nutzen Twitter, Facebook und LinkedIn als unverzichtbares Mittel zur Verbesserung der Kundenbindung, und selbst Entwicklungsabteilungen setzen YouTube zur Vorstellung neuer Produkte ein. Soziale Medien zeigen rasante Wachstumszahlen, die sie unverzichtbar für Unternehmen machen.

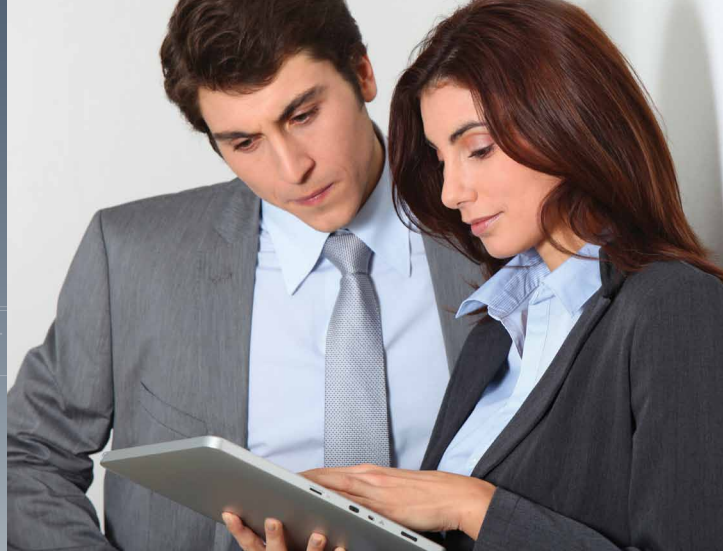
- Facebook hat 750 Millionen Nutzer, die dort monatlich 700 Milliarden Minuten verbringen.[2]
- In Twitter generieren 200 Millionen Nutzer jeden Tag 65 Millionen Tweets.[3]
- Bei LinkedIn sind 100 Millionen Berufstätige aus 1 Million Unternehmen versammelt.[4]
- YouTube hat jeden Monat 490 Millionen Besucher aus der ganzen Welt, die 92 Milliarden Videos aufrufen.[5]

Tatsächlich ist es aber so, dass sich genau die Eigenschaften, die soziale Medien für unser Geschäfts- und Privatleben so attraktiv machen, auch für böswillige Zwecke missbrauchen lassen. Laut einer aktuellen Studie, die McAfee zusammen mit dem internationalen Beratungsunternehmen Vanson Bourne sowie der CERIAS-Gruppe der Purdue University durchführte, werden soziale Medien in Brasilien, Spanien und Indien zu mehr als 90 Prozent eingesetzt, und selbst in den USA, Großbritannien, Australien und Kanada finden sie noch mehr als 70 Prozent Verbreitung. Die Welt ist dank sozialer Medien voller interessanter Ziele. Von den über 1.000 internationalen Unternehmen, die im Rahmen der Studie befragt wurden, sorgte sich die Hälfte beim Einsatz sozialer Medien um die Sicherheit. Ganze 70 Prozent mussten diesbezüglich bereits Sicherheitskompromittierungen wie Malware-Infektionen, Datenverluste oder Phishing-Betrug hinnehmen. Die befragten Unternehmen nannten Verluste von insgesamt mehr als 1 Milliarde US-Dollar durch Zwischenfälle im Zusammenhang mit sozialen Medien.

- Die finanziellen Verluste, die durch Social-Media-Sicherheitsvorfälle entstehen, liegen bei durchschnittlich 2 Millionen US-Dollar.
- Großen Unternehmen entstehen im Durchschnitt finanzielle Verluste von fast 4,5 Millionen US-Dollar.[6]
- 60 Prozent der Unternehmen gaben an, dass der schwerste Schaden im Zusammenhang mit Social-Media-Sicherheitsvorfällen für den Ruf des Unternehmens und den Markennamen entstand. 14 Prozent nannten Kosten durch Gerichtsverfahren.

85 PROZENT

85 Prozent der Unternehmen mit mehr als 1.000 Mitarbeitern setzen derzeit Richtlinien für soziale Medien ein, und 80 Prozent lassen Zugang zu Social-Media-Webseiten zu.[8]



Lösungen

Auf Nutzerseite stehen zahlreiche Möglichkeiten wie Mitarbeiterschulungen und angepasste Richtlinien zur Verfügung, die zur Behebung von Risiken im Zusammenhang mit sozialen Medien herangezogen werden können. Gleichzeitig benötigen Sie technische Lösungen, mit denen Vorfälle vermieden werden können, bei denen Böswilligkeit und Unachtsamkeit im Spiel sind. Zu diesen Lösungen gehören anwendungsbasierte Kontrollen sowie Daten- und Malware-Schutz.

Anwendungsbasierte Kontrollen

Nehmen wir zum Beispiel Facebook. Das Zulassen oder Verweigern des Zugangs zu Facebook ist nicht so einfach wie bei einer statischen Webseite, denn Facebook besteht aus hunderten oder tausenden von Einzelanwendungen. Daher sollten anwendungsbasierte Kontrollen eingesetzt werden, die Zugang zu bestimmten Anwendungen innerhalb von Webseiten zulassen, ihn bei zeitintensiven Anwendungen (z. B. Browser-Spielen) jedoch auch verweigern können. Durch die Integration einer Benutzerdatenbank wie Microsoft Active Directory wäre es außerdem möglich, Regeln für bestimmte Gruppen und Personen festzulegen und so eine differenzierte Kontrolle über die Interaktion der Benutzer mit Social Media-Anwendungen zu erreichen.

Datenschutz

Datenschutz betrifft viele Sicherheitsbereiche, seien es Benutzer (einschließlich System- und Datenbank-Administratoren sowie andere berechtigte Gruppen, die auf Datenbanken, Anwendungen und Dateifreigaben zugreifen können) oder Kopiervorgänge sensibler Daten auf Wechselmedien wie USB-Laufwerke. Wenn jedoch soziale Medien im Spiel sind, ist Datenschutz unverzichtbar beim Schutz von Unternehmen vor der Unachtsamkeit ihrer Mitarbeiter oder anderen Insidern, die sich nicht an Unternehmensrichtlinien halten. Ein Beispiel dafür ist die Veröffentlichung sensibler Informationen wie Personalausweisnummern oder anderen staatlichen Identifikationsinformationen auf Webseiten wie LinkedIn. Daher sollten die eingesetzten Lösungen die Veröffentlichung sensibler Daten registrieren und blockieren können. Außerdem sollten abhängig vom jeweiligen Benutzer einige oder alle Webseiten schreibgeschützt werden. Eine weitere Möglichkeit besteht in der Veränderung der Darstellung bestimmter Seiten, sodass wichtige Funktionen aus der Web-Oberfläche des Benutzers entfernt werden. So könnten zum Beispiel für LinkedIn Kontrollen eingerichtet werden, die bestimmte Funktionen wie Posteingang oder Suchfunktionen im Browser deaktivieren.

Malware-Schutz

Web-Browser wie Microsoft Internet Explorer, Firefox, Safari, Opera und Chrome sind leistungsfähig und komplex. Dies gilt auch für die von ihnen unterstützten Anwendungen wie Java, Flash, Shockwave und Windows Media Player. Da Browser sowie ihre Anwendungen notwendig sind, um heutige Webseiten vollständig nutzen zu können, gibt es keinen Computer, auf dem sie nicht eingesetzt werden. Das macht sie zu einem vorrangigen Ziel. Daten von McAfee® Labs™ zeigen, dass die Anzahl der Malware-Bedrohungen von weniger als 6.000 Exemplaren im Januar 2007 auf mehr als 56 Millionen Varianten im Januar 2011 stieg. Diese erschreckende Zunahme bedeutet, dass herkömmliche signaturbasierte Virenschutz-Lösungen (auch Blacklisting genannt) zwar vor bekannten Bedrohungen schützen, aber nur ungenügenden Schutz vor neuen Bedrohungen bieten, die auf soziale Medien setzen. Daher müssen Malware-Schutzlösungen den Blacklisting-Ansatz um Verhaltensanalysen ergänzen. Die Verhaltensanalyse sollte die Authentifizierung von Code, Medientyp-Überprüfung sowie Kontrollen im Zusammenhang mit Verhalten und Reputation umfassen. Diese Funktionen sind in Verbindung mit Blacklisting in der Lage, bekannte und unbekannte Angriffe auf Betriebssysteme, Browser und die darin ausgeführten Anwendungen abzufangen. Auf diese Weise können gängige Angriffe wie Phishing-Betrug mithilfe sozialer Medien, der zur Kompromittierung des Benutzersystems führt, durch die proaktive Bewertung der Reputation von Webseiten und die Analyse der Dateiparameter abgewehrt werden.

Empfohlene Vorgehensweisen

- Nutzen Sie soziale Medien, um auf dem Markt bestehen zu können. Setzen Sie dabei Sicherheitskontrollen ein, um Risiken zu minimieren.
- Ihre Mitarbeiter müssen sich der Risiken bewusst sein. Achten Sie darauf, dass Ihre Sicherheitsrichtlinien soziale Medien abdecken.
- Implementieren Sie mehrstufige Kontrollen. Obwohl verschiedene Lösungen vor Social-Media-Sicherheitsvorfällen schützen, sind anwendungsbasierte Kontrollen sowie Daten- und Malware-Schutz für den Unternehmenserfolg unverzichtbar.
- Setzen Sie benutzer- und anwendungsbasierte Kontrollen ein. Präzise Anpassbarkeit ist unverzichtbar!
- Setzen Sie zum Schutz vor unachtsamen und böswilligen Benutzern Lösungen ein, die Funktionen zur Filterung, Blockierung und Modifizierung von Online-Aktionen wie Dateneingaben enthalten.
- Durch den Einsatz von Malware-Schutzlösungen, die signaturbasierten Virenschutz mit Verhaltensanalysen ergänzen, können Sie sich vor bekannten und unbekannten Bedrohungen schützen.

55 Prozent der Unternehmen glauben, dass ihre Mitarbeiter versehentlich Malware ins Unternehmen eingelassen haben oder aus Unachtsamkeit für Datenkompromittierungen verantwortlich waren.[9]

Wertsteigernde Faktoren

Einer der wichtigsten Sicherheits-Aspekte sozialer Medien ist die unerwünschte oder versehentliche Kompromittierung sensibler Daten.

- Der Wert Ihres Engagements bei sozialen Medien berechnet sich in erster Linie aus den Kosten für den Verlust wichtiger Daten sowie der subjektiven Steigerung der Benutzerproduktivität. McAfee-Lösungen unterstützen Sie dabei, Ihre Mitarbeiter in diesem besonders sensiblen Bereich zu kontrollieren und zu verwalten. Außerdem können Sie dadurch ausreichende Compliance-Bemühungen nachweisen.
- Der Einsatz sozialer Medien kann zudem Ihren Mitarbeitern zeigen, dass Ihr Unternehmen innovativ genug ist, um neue Möglichkeiten einzusetzen, dabei jedoch kontrolliert und überlegt vorzugehen.

Dazugehöriges Material aus der McAfee Security Connected-Referenzarchitektur

Stufe II
- Schutz mobiler Geräte
- Ermöglichung der Konsumerisierung von Mitarbeitern
- Schutz von Informationen

Stufe III
- Schutz Cloud-basierter Kommunikation
- Nutzung des BYOPC-Prinzips (Bring Your Own PC)
- Erzwingung von Endgeräte-Compliance
- Schutz und Kontrolle von Laptops

Weitere Informationen zur Security Connected-Referenzarchitektur finden Sie unter: http://www.mcafee.com/de/enterprise/reference-architecture/index.aspx.

Informationen zum Autor

Brian Contos ist zertifizierter IT-Sicherheitsexperte (CISSP) und Director of Global Security Strategy bei McAfee. Er ist anerkannter Sicherheitsexperte mit fast zwanzig Jahren Erfahrung in den Bereichen Sicherheitstechnologien und -Management. Contos ist Autor mehrerer Bücher, einschließlich *Enemy at the Water Cooler* (Feind am Wasserkühler) und *Physical and Logical Security Convergence* (Physische und logische Konvergenz der Sicherheit). Er war für Regierungsunternehmen sowie Forbes Global 2000-Unternehmen in Nord-, Mittel- und Südamerika, Europa, Asien und im Nahen Osten tätig. Contos ist gern gesehener Redner bei bedeutenden Veranstaltungen der Branche wie RSA, Interop, SANS, OWASP und SecTor und Autor von Artikeln für Branchen- und Wirtschaftsblätter wie *Forbes*, *New York Times* und *The Times of London*. Er ist Distinguished Fellow am Ponemon Institute und Absolvent der University of Arizona.

brian_contos@mcafee.com || http://siblog.mcafee.com/author/brian-contos/ || @BrianContos

[1] http://www.gartner.com/it/page.jsp?id=1467313
[2] http://www.cedmag.com/article-detail.cfm?id=10926254
[3] ebda.
[4] ebda.
[5] ebda.
[6] ebda.
[7] ebda.
[8] http://www.scribd.com/doc/54161974/Wired-Workforce-Networked-CSR-Final
[9] http://www.mcafee.com/de/resources/data-sheets/ds-host-data-loss-prevention.pdf

McAfee An Intel Company

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de