

Worauf Unternehmen 2009 besonders achten müssen

Die drei Trends der Web-Kriminalität

Die Guten werden zu den Bösen, Browser als Betriebssysteme und falsche Identitäten in sozialen Netzwerken: Die drei größten Bedrohungen für die Web-Sicherheit 2009.

Die Internet-Kriminalität wandelt sich. Klassische technische Attacks lassen nach. "Der Trend geht zu social attacks", sagt Ian Amit, Director of Security Research beim Sicherheitsanbieter Aladdin. Im "Annual Threat Report" nennt er drei Bedrohungen, die dieses Jahr die [Web-Kriminalität bestimmen](#) (<http://www.cio.de/knowledgecenter/security/859182/index2.html>) und die sich Unternehmen bewusst machen sollten:

› **1. Datendiebstahl durch eigene Mitarbeiter**

Die Wirtschaftskrise, ein Immobilienmarkt im freien Fall und ein angespannter Arbeitsmarkt führen dazu, dass die Online-Kriminalität steigt. Mit steigendem Druck werden Unternehmen zunehmend versuchen, [Personal von Konkurrenten zu rekrutieren](#) (<http://www.cio.de/financeit/analysen/840073/>). Ziel ist es, an wichtige Geschäftsdaten zu kommen.

Das betrifft besonders den Finanzsektor. Schließlich spüren Banken die Auswirkungen der Krise am meisten. Der Report geht davon aus, dass Kriminelle versuchen, nicht mehr nur technische Mitarbeiter anzuwerben, sondern auch Manager, die so ihr Gehalt aufstocken wollen.

› **2. Unsichere Anwendungen bei Browsern als Betriebssystem**

Mit der Verbreitung von Web 2.0 werden sich die Anwendungen des Internets zunehmend verändern. Wie Google Chrome zeigt, kann sich der Browser mit der richtigen Kombination von optimierten Web-2.0-Technologien in ein vollständiges Betriebssystem verwandeln.

Mit den bereits integrierten Gears-Technologien von Google wäre es laut Amit nicht überraschend, wenn ein Adobe-Air-Fähiger Browser auf den Markt kommt, der eine verbesserte Desktop-Web-Integration bietet. Außerdem zu erwarten sind 2009 leistungsfähige Betriebssystem-Browser von Microsoft.

Mit dem technischen [Fortschritt lauern aber auch die Gefahren](#) (<http://www.cio.de/knowledgecenter/security/865561/>). Vorsicht ist besonders bei mobilen Geräten wie [Netbooks oder iPhones](#) (<http://www.cio.de/index.cfm?pid=415&pk=866067>) geboten. Immer mehr Anwendungen werden nur noch übers Web laufen. Sie sind deshalb einem höheren Risiko von Attacks ausgesetzt. Unternehmen, bei denen mobile Geräte zum Einsatz kommen sollen, müssen sich die Herausforderungen an die Sicherheit bewusst machen.

› **3. Gefahr durch Social Networking**

Da immer mehr Mitarbeiter und Unternehmen [Social Networking](#) (<http://www.cio.de/knowledgecenter/security/847527/index2.html>) betreiben, steigt der Wert von Web-Identitäten für kriminelle. Öffentlich zugängliche Daten auf Portalen wie Facebook oder LinkedIn machen es ihnen einfach, Identitäten zu imitieren, zu zerstören oder falsch darzustellen.

Aber auch wer sich nicht am Social Networking beteiligt, läuft Gefahr Opfer zu werden. "Mit den Informationen, die ich über eine Person bei Google finde, erstelle ich in kürzester Zeit ein Profil für jemanden anderen", sagt Amit.

Er prognostiziert eine Zunahme von Identitätsraub im Web. Bis es zu einer Verschärfung der Anforderungen zur Verifizierung von Identitäten kommt, rät der Experte zur Vorsicht.

Auch wenn es auf Andere Eindruck macht, viele Kontakte auf Network-Seiten zu haben, sollte nicht jedes Angebot ungeprüft in die Liste aufgenommen werden. Außerdem: Lieber ein eigenes Profil mit wenig Informationen erstellen und dieses selbst kontrollieren, bevor sich jemand anderes für einen ausgibt.

› **Forschungsergebnisse des Attack Intelligence Center**

Der "Annual Threat Report" von Aladdin ist eine Zusammenfassung der Forschungsergebnisse des Attack Intelligence Center. Er macht auf Bedrohungen aufmerksam, will aber keine konkreten technischen Lösungen liefern.

Autor(en): Alexander Galdy

IDG Business Verlag GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Verlag GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in CIO unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von CIO aus gelinkt wird, übernimmt die IDG Business Verlag GmbH keine Verantwortung.