

Sicherheitshinweis: Webseite von Torrentreactor manipuliert

Schadsoftware kann über viele Wege in den eigenen Rechner gelangen. In grauer Vorzeit wurde Viren über Disketten verbreitet, später und bis heute über E-Mail-Anhänge. Aktuell sind Bedrohungen durch sogenannte Drive-by-Downloads, bei denen beim Besuch von Webseiten nicht nur die gewünschten Texte, Graphiken, Videos und Flash-Animationen, sondern en passant noch weitere (ungewollte oder schädliche) Dateien auf den Rechner übertragen werden. Möglich ist dies durch die dynamische Gestaltung von Webseiten (Stichworte Javascript, Flash, Ajax), die während des Ladens und Betrachtens einer Webseite im Hintergrund eine Vielzahl von Kommunikationsvorgängen ermöglicht. Ist eine Webseite „verseucht“, so wird dabei auch Schadcode übertragen. In Kombination mit einer Sicherheitslücke des Browser kann dieser Schadcode die Browser-Sicherheitsmechanismen überwinden und sich auf dem Betriebssystem des Benutzers einrichten - der Rechner ist verseucht.

War früher die Gefahr in den „dunklen Ecken“ des Internets konzentriert, so ist heutzutage auch auf renommierte Webseiten Schadcode zu finden: Hintergrund ist hier, dass die Software der Webserver

und Content-Management-Systeme für Webinhalte nicht fehlerfrei ist und Sicherheitslücken von Dritten ausgenutzt werden, indem sie den Schadcode auf den Servern der renommierten Webseitenbetreiber einschleusen, die ihn dann an ihre Benutzer weiterreichen.

Genau solch eine Manipulation meldet die Firma Websense Security Labs Anfang Juli: Auf der Webseite von Torrentreactor, einer bekannten Suchmaschine für das Torrent-Netzwerk, wurde ein solcher Schadcode gefunden. Heutzutage hilft die firmenweite Beschränkung des Webseitenzugriffs auf „sichere“ Seiten (sogenanntes White-Listing) nicht weiter, denn jede „sichere Seite“ kann unbemerkt gehackt und kontaminiert werden. Schutz versprechen eher sorgfältiges Patchen der Browser und Browser-Plugins (etwa für Flash-Animationen, pdf-Darstellung, etc.) sowie zentrale oder dezentrale Webfilter, die die Webinhalte auf Schadcode analysieren. ■ TP

Internet: <http://securitylabs.websense.com/content/Alerts/3430.aspx>

Stichworte: Schadsoftware, Drive-by-Download, Torrentreactor, Torrent, Internet-Sicherheit

Mit Biometrie im Handumdrehen zum Passwort-Reset

Wird ein Passwort mehrfach falsch eingegeben und eine Anwendung dadurch gesperrt, muss der Zugangscode zurückgesetzt werden. Das ist umständlich und kostet Zeit. Erleichterung und Kosteneinsparung versprechen Systeme, die - automatisiert - mit biometrischer Sprach- und Stimmerkennung arbeiten.

Von **BERND HOHGRÄFE** und **SEBASTIAN JACOBI**, Essen.*

Passwörter sind praktisch und werden vielfach eingesetzt. Die Anzahl der Passwörter, die Benutzer privat und beruflich verwenden, nimmt damit ständig zu - und damit passiert es gelegentlich, dass ein Passwort vergessen wird. Gelegentlich aus Sicht des Benutzers, (zu) häufig aus Sicht des Unternehmens, dessen User-Helpdesk die Passwörter zurücksetzen muss. Die Erfahrung zeigt, dass jeder User mindestens einmal jährlich davon betroffen ist. Benutzer, die ihre Passwörter für bestimmte Applikationen gemäß der vorhandenen Policies regelmäßig ändern müssen, haben ein weiteres

Problem: Sie können sich aus Applikationen ausperren, wenn sie mehrfach ein falsches Passwort eingegeben haben. Die meisten User vertrauen dazu nämlich auf Varianten eines Standardpasswortes. Doch manchmal können sie sich nicht mehr daran erinnern, welche ihrer Varianten sie für eine Anwendung zuletzt vergeben haben. Manchmal führen aber auch versehentlich arretierte Num-Lock- oder Caps-Lock-Tasten zur falschen Eingabe, insbesondere, da Passwörter heute oft zwingend Sonderzeichen und Ziffern enthalten müssen. Solche Vorfälle passieren – zumindest nach subjektivem Empfinden der Benutzer – meist kurz vor Feierabend, auf Geschäftsreise, abends oder am Wochenende im Home Office, wenn es eilt und keine Hilfe zu erwarten ist. Dies ist auch aus Unternehmenssicht kritisch, wenn Mitarbeiter unbedingt terminkritische Arbeiten rechtzeitig fertig stellen müssen, um zum Beispiel Fristen für eine Ausschreibung oder ein Angebot einzuhalten.

Vergessen kann teuer werden

Aber auch innerhalb der normalen Arbeitszeit ent-