Studie: Reale Gefahren in virtuellen Welten

Die europäische Sicherheitsagentur ENISA warnt in einer Studie vor Identitätsdiebstahl und anderen Umtrieben in virtuellen Welten oder Multiplayer-Universen.

die Meldung vom 20.11.2008

Der Verlust von echtem Geld und persönlichen Daten sind eine Realität in virtuellen Welten. Die European Network and Information Security Agency (ENISA) warnt auf der Basis einer heute veröffentlichten Studie (PDF-Datei) vor zahlreichen Risiken in virtuellen Welten und so genannten Massive Multiplayer Online Games (MMO) wie World of Warcraft. Insgesamt geht die europäische Netzsicherheitsbehörde von einem extremen Anstieg von Betrugsfällen in den virtuellen Welten aus. Eine Umfrage (PDF-Datei) der Agentur unter 1500 Nutzern ergab, dass rund ein Drittel in jüngster Zeit um ihr virtuelles Eigentum gebracht wurden.

Verkaufserlöse für virtuelle Objekte von geschätzten 2 Milliarden US-Dollar im Jahr 2007 und die von den Kaspersky Labs gemeldete Zunahme von Schadsoftware illustriert nach Ansicht von ENISA die Bedeutung des Problems. "Das Versäumnis, die Bedeutsamkeit von Schutzmechanismen für Geldwerte in dieser Grauzone der Wirtschaft anzuerkennen, hat 2007 zum Jahr des Betrugs in Online-Welten gemacht", warnt die Agentur. Der Bericht beschreibt 14 Bedrohungsszenarien. An oberster Stelle rangiert der Identitätsdiebstahl, um an virtuelles Eigentum oder echtes Geld eines Spielers zu gelangen. Auch geistiges Eigentum, so die ENISA-Autoren, sei in virtuellen Welten nicht sicher.

Der Diebstahl persönlicher Daten werde den Angreifern in der virtuellen Welt besonders leicht gemacht. "Avatare unterscheiden sich nicht von anderen Online-Identitäten. Nutzer neigen dazu, sogar mehr persönliche Daten preiszugeben, da sie sich innerhalb von virtuellen Welten in einer trügerischen Sicherheit wähnen." Es gebe bereits einen Trend, das Abhören von Avataren für Marketingzwecke einzusetzen. Nicht zuletzt warnt die Studie vor möglichem Stalking und Belästigung in den virtuellen Welten.

Weitere Risiken betreffen klassische, technische Angriffszenarien wie Denial of Serivce Attacken, die angesichts zentraler Infrastrukturen besonders einfach sind. Die Automatisierung bestimmter Funktionen könne von Angreifern ausgenutzt werden, um sich (manchmal geldwerte) Vorteile zu verschaffen. XML, HTTP oder RPC-Requests können für Portscans oder Spamming missbraucht werden. Skripting etwa mit Befehlen wie "LlGetLandOwnerAt" in Second Life erlaube es Angreifern, massenhaft und gezielt persönlichen oder wirtschaftlich bedeutsame Daten zu sammeln.

Die Studie schließt mit Handlungsempfehlungen an Regierungen und Regulierer sowie die Anbieter selbst. Regierungen sollten demnach ein Forum für die Betreiber einrichten, über das diese Erfahrungen austauschen können. ENISA bietet an, den konkurrierenden Anbietern einen neutrales Forum zu bieten. Regierungen sollten gleichzeitig in die Klärung relevanter Rechtsfragen investieren, etwa den Status personenbezogener Daten oder geistigen Eigentums in virtuellen Welten betreffend. Weiterhin sollten unabhängige Schlichtungsverfahren für die Spiele-Teilnehmer gefördert werden.

Die Anbieter selbst sollten zunächst bestehende technischen Gefahren minimieren und für mehr Sicherheit bei Nutzertransaktionen sorgen. Außerdem gelte es die spezifischen DDOS-Attacken zu bekämpfen. Oftmals seien rasche Gegenmaßnahmen

im Ernstfall erfolgversprechender als Vorbeugung, meint man bei ENISA. Jegliche Maßnahme zur besseren Authentifizierung von Nutzern sei darüber hinaus begrüßenswert. Eine Boot-CD könne kritische Operationen – etwa finanzielle Transaktionen – besser absichern.

Datenschutzregeln sollten schließlich für die Nutzer klarstellen, wo welche Daten erfasst werden und was von anderen Nutzern leicht belauscht werden kann. Alle Regeln sollten zusammengefasst an einer Stelle abrufbar sein.

(Monika Ermert) / (vbr / c't)