

Aktuelle Meldung

Hochsichere Datenschleuse erleichtert Umstieg auf neuen Internet-Standard

7. Januar 2010

Potsdam. Die von Forschern des Hasso-Plattner-Instituts entwickelte Hochsicherheitsschleuse „Lock-Keeper“ kann jetzt auch den Datenfluss zwischen zwei Netzwerken regeln, von denen eins nach dem alten Internetprotokoll IPv4 und das andere nach dem neuen Standard IPv6 funktioniert. Das teilte Institutsdirektor Prof. Christoph Meinel mit. Das Hardware-basierte Rechnersystem Lock-Keeper schützt Netzwerke von Unternehmen oder Behörden durch physikalische Trennung vom Internet vor Angriffen. Gleichzeitig ermöglicht die Datenschleuse sicheren Nachrichtenaustausch zwischen den Netzen.

Dank einer Erweiterung ist der Lock-Keeper nun zum Beispiel in der Lage, ein nach dem neuen Standard IPv6 funktionierendes Intranet einer Behörde oder eines Unternehmens mit dem Internet zu verbinden, in dem noch das Protokoll IPv4 angewendet wird. „Das System fungiert somit als Übersetzer zwischen den Protokollen“, erläuterte Meinel. Interessant sei es zum Beispiel für alle öffentlichen Verwaltungen in Deutschland, die künftig in ihren Netzen auf den neuen Internetstandard IPv6 umstellten, fügte Meinel hinzu. Vertrieben wird die Hochsicherheitsschleuse von der Siemens AG Schweiz.

„Der Lock-Keeper beruht auf dem einfachen Prinzip, dass man ein Netzwerk am besten schützt, wenn man es von anderen getrennt hält“, berichtete Meinel, der auch Leiter des HPI-Fachgebiets Internet-Technologien und -Systeme ist. Durch die patentierte Technologie kann erreicht werden, dass Netzwerke höchstmöglich vor Online-Angriffen geschützt und sensible Daten gegen Internet-Spionage gesichert werden. „Daten, die vom einen Netz ins andere wollen, werden zunächst in den Lock-Keeper übertragen und können dort auf bösartigen Code und Schadsoftware geprüft werden, bevor sie dann sicher in das geschützte Netz übermittelt werden“, erläuterte der Wissenschaftler das Funktionsprinzip.

„Erreicht wird das höchstmögliche Sicherheitsniveau durch die vollkommene physikalische Trennung. Der Lock-Keeper sorgt dafür, dass zu keinem Zeitpunkt eine Verbindung zwischen den beteiligten Netzwerken besteht“, betonte Meinel. Zuverlässig unterbunden werden nach seinen Worten somit alle online-basierten Angriffe durch Spyware, Backdoors, Angriffe auf der Protokollebene wie etwa TCP Sequence Number Attack, Tunneling oder Fragmentation Attacks.

PRESSEMITTEILUNG

Denial of Service Angriffe werden so abgeblockt, dass sie das zu schützende Netz nicht beeinträchtigen können. „Anders als bekannte Schutzmechanismen, wehrt der Lock-Keeper proaktiv auch bislang unbekannte Angriffsarten ab, die auf eine bestehende Verbindung der Netze angewiesen sind“, hebt der Wissenschaftler einen besonderen Vorteil hervor. Durch die Implementierung bestimmter Trusted Computing-Konzepte erfüllt der Lock-Keeper die Anforderungen von Institutionen mit höchstem Bedarf an Sicherheit vollständig. Dazu gehören Militär, Polizei und andere Sicherheitsbehörden genauso wie etwa Finanzdienstleister und Unternehmen der Energieversorgung, des Bereichs Telekommunikation, des Transportsektors und der Luft- und Raumfahrt.

Pressekontakt: Telefon: 0331 55 09-150, Mail: presse@hpi.uni-potsdam.de

Hans-Joachim Allgaier, Tel.: 0331 55 09-119,

AllgaierCommunication: Tel.: 06081 57 76 30, Mobil: 0179 267 54 66,

Fax: 06081 96 25 17,

Mail: allgaier@hpi.uni-potsdam.de, info@allgaiercommunication.de

Kontakt für Fotos, Illustrationen und Logos:

Katrin Augustin, Hasso-Plattner-Institut,

Fax: 0331 55 09-169, Mail: katrin.augustin@hpi.uni-potsdam.de