Die Gefahren von BMC und IPMI: Raritan warnt vor häufigen Schwachstellen

Die Gefahren von BMC und IPMI: Raritan warnt vor häufigen Schwachstellen

Fremdzugriff auf den unternehmenseigenen Server verhindern
Unternehmen nutzen beim Remote-Server-Management so genannte Baseboard Management Controller (BMC) sowie die dazugehörigen Intelligent Platform Management Interface (IPMI)-Protokolle. Die BMCs haben direkten Zugriff auf das Motherboard des Servers. Dadurch ist es dem Tool möglich, den Server zu überwachen, zu booten und sogar neu zu installieren. Durch den KVM-over-IP-Zugriff sowie die Verbindung zu Remote-Medien können Nutzer eines BMC einen Server auch aus der Ferne bedienen. Aktuell tauchen jedoch vermehrt Schwachstellen bei BMCs und IPMI auf. Data Center-Experte Raritan warnt daher vor Schwachstellen, die Fremdzugriffe auf den Firmenserver zur Folge haben können.
Die Schwachstellen, die bei BMCs auftraten, wurden hauptsächlich von zwei Security-Experten identifiziert: Dan Farmer, ein Pionier in der Entwicklung der Schwachstellen-Scanner, entdeckte und dokumentierte die Schwachstellen ursprünglich; H. D. Moore (Entwickler der Netzwerk-Security-Software Metasploit Framework) beschrieb, wie man die Schwachstellen mit schnell verfügbaren Sicherheits-Tools erkennen kann. Moore entdeckte darüber hinaus mehr als 300.000 IPMI-fähige, leicht angreifbare Server, die mit dem Internet verbunden waren. Diese Server offenbarten ebenfalls einige Schwachstellen.
Wo eine Schwachstelle, da auch ein Angriff
BMC- und IPMI-Schwachstellen haben Folgen für Unternehmen und Organisationen: Die Cyper 0-Authentifizierung der BMCs funktioniert mittels Passwort-Zugriff. Jedoch können die BMC-Passwort-Hashes durch Brute Force-Methoden geknackt werden. Die Cyberkriminellen nutzen dafür einfach die auftretenden Schwachstellen aus. Ebenso angreifbar sind BMCs mit aktiviertem "anonymous"-Zugang.
Zudem traten in der Vergangenheit vermehrt UPnP (Universal Plug and Play)-Schwachstellen auf, die Root-Zugriffe auf den BMC sowie das Entwenden von Klartext-Passwörtern ermöglichten. Sobald der BMC geknackt wird, gibt es also viele Möglichkeiten, ihn anzugreifen, zu kontrollieren und den Server in Beschlag zu nehmen. Umgekehrt kann der BMC genutzt werden, um bei einem kompromittierten Server ein Backdoor-Benutzerkonto einzurichten.
Schwachstellen beim BMC sofort melden
Allen Server-Administratoren und Sicherheitsbeauftragten muss bewusst sein, dass die von Farmer und Moore erkannten Schwachstellen auch ihre Server betreffen können. Sobald sich ihre IPMI- und BMC-Implementierungen verändern, sollten Anwender den Server-Hersteller konsultieren. Farmer bietet verunsicherten Usern darüber hinaus Best Practices in puncto IPMI-Security an, während ihnen Moore nützliche FAQs zur Verfügung stellt.
Obwohl die Schwachstellenforschung bezüglich BMC und IPMI noch ziemlich neu und nicht vollständig ausgereift ist, sind sich die RZ-Experten von Raritan trotzdem einig, dass Kunden die Schwachstellen ernst nehmen sollten. Angesichts der hohen Bedeutung des BMC für die Unternehmensserver ist dies doppelt wichtig.
Gefahren für Netzwerke ins Auge blicken
"Neben den Schwachstellen im IPMI-Protokoll scheinen auch die dazugehörigen Geräte der meisten BMCs ähnliche Probleme zu haben", erklärt Moore. "Zu den Problemquellen zählen Standard-Passwörter, veraltete Open-Source-Software und in einigen Fällen Backdoor-Konten sowie statische Verschlüsselungs-Keys. Die Welt der BMCs ist ein Durcheinander, das sich wahrscheinlich auch nicht allzu bald bessern wird. Wir müssen uns demnach den Gefahren dieser Geräte für unsere Netzwerke bewusst sein."
"Stellen Sie sich vor, Sie versuchen einen Computer abzusichern, der einen kleinen störenden Server auf dem Motherboard hat; quasi einen Blutsauger, der weder ausgeschaltet noch dokumentiert werden kann", erläutert Farmer. "Sie können sich nicht einloggen, keine Patches einpflegen oder Probleme beheben. Zudem können sie keine Server-basierten Abwehrmechanismen, Audits oder Anti-Malware-Software nutzen. Die Konstruktion des Servers ist undurchsichtig und die Implementierung schon alt. Dies ist die perfekte Plattform zum Spionieren, fast unsichtbar dem Host gegenüber. Der Blutsauger hat also die volle Kontrolle über die Hard- und Software des Computers. Für so eine Remote-Kontrolle und -Überwachung wurde er sogar speziell ausgerichtet."
Weitere Informationen unter www.raritan.de .
Informationen zu Raritan
Die Raritan Deutschland GmbH mit Sitz in Essen ist Hersteller und Anbieter in den Bereichen Power Management, sicheres Infrastrukturmanagement, KVM und serielle Lösungen für Rechenzentren jeder Größe. Das Unternehmen unterstützt seine Kunden von der Planung über die Integration bis zum Betrieb. Seinen Hauptsitz hat Raritan in Sommerset/New Jersey mit weltweit 38 Niederlassungen. Zu den intelligenten Power Management-Lösungen zählen die Produktfamilie "Dominion PX" mit hunderten Modellen für jede Anforderung sowie Power IQ - eine intuitive Software zur Datenauswertung über ein zentrales Web-Interface. IT-Administratoren und Facility Manager können mit diesen Lösungen Stromverbrauch sowie Stromzufuhr am Rack überwachen und uneingeschränkt steuern. Zum Produktangebot zählen außerdem Geräte für den KVM-over-IP- oder Serial-over-IP-Zugriff sowie leistungsfähige Echtzeit-Managementsoftware für Rechenzentren. Die mehrfach ausgezeichneten Raritan Power- und Access
Control-Produkte tragen maßgeblich dazu bei, dass die Produktivität in Rechenzentren gesteigert und Geschäftsprozesse in einzelnen Niederlassungen erweitert werden. Die Raritan Deutschland GmbH ist Mitglied im Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und dort im Green-IT-Anbieterverzeichnis gelistet. Darüber hinaus ist Raritan Mitglied im eco, dem Verband der deutschen Internetwirtschaft e.V. Weitere Informationen finden Sie unter www.raritan.de .

Raritan Deutschland GmbH
Lazarettstr. 7-9
D-45127 Essen
Mareike Wondzenski
Tel.: +49 (0)201 747 98-0
Fax: +49 (0)201 747 98-50
E-Mail: mareike.wondzenski@raritan.com
 www.raritan.de
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: oh@sprengel-pr.com
 ms@sprengel-pr.com
 www.sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=544280" width="1" height="1">

Pressekontakt

Raritan

45127 Essen

mareike.wondzenski@raritan.com

Firmenkontakt

Raritan

45127 Essen

mareike.wondzenski@raritan.com

Informationen zu RaritanRaritan ist ein Hersteller und Anbieter in den Bereichen Power Management, sicheres Infrastrukturmanagement, KVM und serielle Lösungen für Rechenzentren jeder Größe. Das Unternehmen unterstützt seine Kunden von der Planung über die Integration bis zum Betrieb. Zu den intelligenten Power Management-Lösungen zählen die Produktfamilie ?Dominion PX mit hunderten Modellen für jede Anforderung sowie Power IQ ? eine intuitive Software zur Datenauswertung über ein zentrales Web-Interface. Mit diesen Lösungen sind IT-Administratoren und Facility Manager in der Lage, den Stromverbrauch und die Stromzufuhr am Rack zu überwachen sowie vollständig zu steuern. Das Produktangebot umfasst zudem Geräte für den KVM-over-IP- oder Serial-over-IP-Zugriff sowie leistungsfähige Echtzeit-Managementsoftware für Rechenzentren. Die Raritan Power- und Access&Control-Produkte sind bereits mehrfach ausgezeichnet worden. IT-Verantwortliche, -Führungskräfte und Administratoren erhalten so gezielt Kontrollmöglichkeiten zur Verbesserung ihrer Energieeffizienz, Steigerung der Produktivität in ihrem Rechenzentrum und zur Erweiterung von Geschäftsprozessen in einzelnen Niederlassungen. Raritan hat seinen Hauptsitz in Sommerset/New Jersey und betreibt weltweit 38 Niederlassungen. Von dort aus unterstützt Raritan seine Kunden in 76 Ländern und an mehr als 50.000 Standorten weltweit bei der Überwachung und Administration des Serverzugriffs sowie einer intelligenten Stromverbrauchsmessung und Dokumentation. Weitere Informationen finden Sie unter www.raritan.de. Raritan ist Mitglied der BITKOM und engagiert sich im Green Grid, bei der Climate Savers Computing Initiative und im LEED (Leadership in Energy and Environmental Design). Vor Kurzem wurde das Unternehmen von der US-Umweltschutzbehörde EPA für seinen Beitrag zu deren Rechenzentrumsinitiative gewürdigt.