Sony PSN hit by mass password attack

Aussie "family" social network fails security basics

Flash exploits increase 40 fold in 2011

IPv6 security: Everything old is new again

Forget new threats: It's the old-school attacks that keep getting you

Taylor Armerding (CSO (US)) — *22 October, 2011 01:22*

Everybody in IT knows it is a dangerous world out there, filled with an endless variety of cyber attacks aimed at compromising and taking advantage of security flaws.

But there is still a persistent lack of awareness of specific threats and how best to confront them, according to Rob Havelt, director of penetration testing for Trustwave, an international provider of information security and compliance solutions.

The irony, he says, is that it is not necessarily the newest, scariest malware or hack technique that can compromise an enterprise.

CSO's Daily Dashboard gives you a one-stop view of latest business threats. We created it for you! Bookmark it! Use it!

"You see people get whipped up into a frenzy about the latest technique that requires all kinds of technical skill to exploit," he says, "while ignoring stuff that has been around since forever. One of the most common things we find on an internal network is bad password policy -- egregious things like 'admin' for an administrative password, or that the system administration password is blank."

Havelt wrote most of "Earth vs. The Giant Spider: Amazingly True Stories of Real Penetration Tests," which Trustwave members presented at SecTor 2011 in Toronto earlier this week. He says one of the things he urges IT leaders to realize is that a "tiny flaw," like a master default password for a PBX exchange can be "blown up into something that has a serious impact."

That, in fact, is one of his amazingly true stories. Havelt was doing a penetration test of what he describes as a "very secure" Fortune 500 financial company with an older Siemens Rolm PBX telephone exchange. While most of the default passwords had been changed, "one account they hadn't changed, which gave us better than administrative access, so we could use it to become any user."

Havelt and his team cloned mailboxes from the company's help desk, which gave them access to any voice mail.

"While we were testing, a new voice mail came in from somebody on the road, whose VPN access wasn't working. I knew how to fix it, so I called the guy and he gave me his user name, token pin and

RELATED STORIES

Auditing Cloud Services

IPv6 boosts schools' on-net security

568 reasons First State Super's security breach should worry you

Companies shun, hide IPv6 rollouts due to security fears

Australian organisations hit by RSA SecurID attackers

MOST READ

1 Lethal medical device hack taken to next level

2 568 reasons First State Super's security breach should worry you

3 Australian organisations hit by RSA SecurID attackers

4 Siri open to anyone even when iPhone 4S locked

5 Android antivirus king moves on iOS

CSO DIRECTORY more »

Content Security - eSafe

When it comes to content

domain password. I helped him fix his problem, but with a single domain password, it's very easy to escalate your privileges. From there, we got into wealth management and the Department of Homeland Security Watch List," he says.

"All from a phone call."

Get your morning news fix with the daily Salted Hash e-newsletter! Sign up today.

In another case, Havelt and his team were able to hack into a large manufacturer's HD security cameras. Since they could control them, and since five or six of them were pointed at desks, "and they have this 10X optical zoom, we could zoom in on keyboards and desks, harvest passwords and log into other systems."

Sometimes, the vulnerabilities are, or should be, ridiculously obvious. "Things like user names and passwords that are the same, or a network account with a password of 'admin,'" he says.

"I wish I could tell you that these are isolated instances, but they're not. There are thousands of cases."

So what should the prudent IT manager do? Havelt says one problem is that "there are an inordinate number of organizations that are opposed to real pen testing. They try to limit it to a couple of machines at specific times. That's not how attacks work.

"I understand the realities of business," he says. "But it's like going to a doctor for a complete physical and telling him only to look at your hands."

Beyond that, Havelt says better security requires, "carrying things out to their logical conclusion -- looking at a vulnerability and thinking about what can be done with it."

Or, as a recently departed genius CEO was fond of saying: "Think different."

Tags: security

Comments

Post new comment

NAME

EMAIL ADDRESS

The content of this field is kept private and will not be shown publicly.

COMMENT

Users posting comments agree to the CSO comments policy.

Post Preview

Login or register to link comments to your user profile, or you may also post a comment without being logged in.

security, it is essential to stay ahead of the times in delivering new features and functions for a more secure email and web gateway.

MEDIA RELEASES

Sourcefire to Extend Intrusion Prevention to Red Hat Enterprise Virtualisation Platform

Don't Bet your Personal Details on the Melbourne Cup: 10 Winning Tips from AVG (AU/NZ)

Websense Security Survey: IT Stresses as Data Breaches Put Jobs on the Line

Sophos recognised for providing top customer service and support

WatchGuard Extends Business Security with Virtualisation

More Media Releases »

LATEST JOBS

- FTNBN National Project Manager FTTH**VIC**
- FTSenior Technical Support Consultant**NSW**
- FTTechnical Writer**NSW**
- CCSAP Administrator**WA**
- FTExceptional .Net Developer**SA**
- CCIntermediate Web Developer**QLD**
- CC.Net Analyst Programmer**SA**
- FTSystems Lead**VIC**
- FTSoftware Development Manager**QLD**
- FTDUMMY Voice Engineer**WA**
- FTFrontend Developer - HTML5/CSS

SOLUTION CENTERS

Sophos Security Zone

Trend Micro Security Zone

NetIQ Security Zone

Juniper Security Zone

SECURITY AWARENESS TIP

Use It, Don't Lose It: Keeping Your Business Data Safe

Acronis backup tips to keep your business data safe:

Cover all your bases. Make sure your backup will protect all your important data – not just your business documents and files, but critical applications and your email too. Look for a solution that backs up the complete machine along with files and folders.

Don't rely on people power – when you're busy it's easy to overlook, forget or put off backups until 'tomorrow' – of course, tomorrow never comes! Look for a 'set and forget' backup solution that will automatically do a lot of the work for you.

Don't assume, check. Don't assume your backups are working properly.

Recovery test: Try testing your backup. There's nothing worse than discovering your backup hasn't worked!

Check backups automatically: Your software should automatically validate your backed up data.

For the full list of tips

SECURITY ABC GUIDES more »

Cloud architecture: More questions to ask a provider

This is a continuation of the previous cloud deployment article where I created architectural questions that enable a consultant to understand what products are used to support a corporation's top 10 critical applications. Once these product lists are created, it is much easier to map private or public cloud products that can support these same applications.

Read More

Market Place