Can Your Security Keep Up With 70,000 New Malware Strains a Day?

Get Ready for Top 2012 Security Trends: Smartphones, Social Media and the Cloud

IT security has never been simple, but the challenges you face now are more complex than ever. More than half of employees use their own mobile devices for business, and mobile malware is surging. Social technologies are now vital business tools—and a popular vector for spam and phishing. Cloud computing offers new models for growth and innovation but complicates data protection.

Forrester Research Inc. focused on these challenges in its 2011 security strategy report,[1] and heading into 2012, they continue to dominate an evolving security landscape.

- **6 million+** unique malware samples were identified in the first quarter of 2011, a 26% increase from Q1 of 2010 and far exceeding any first quarter in malware history.[2]
- **70,000** new malware strains are detected every day.[3]
- **54% of employees** use their own mobile devices for business purposes.[4]
- **34 million** information workers have installed unsupported software in the past year.[1]
- **63% of businesses** in one recent study said employees' use of social media puts their organization's security at risk.[5]

How can you keep up with these moving targets?

You can't simply lock everything down. As Forrester noted in its report, "Empowered employees can't wait for a two-month risk assessment or adhere to policies blocking legitimate use of social media or limiting their options for mobility just because the security team can't find a solution for them."

Peter Brecl, CenturyLink product manager and security specialist, says, "The challenge is always giving users the flexibility to work effectively while mitigating the risk of exposure you have by allowing that flexibility."

Malware and the malicious websites that distribute it through phishing and spam are still top concerns. And, in many cases, malware finds its way in through the applications users rely on every day: Internet browsers, Java, and Adobe Flash and Acrobat Reader are among the most popular vehicles. But Brecl said the most significant change in 2011—which will only intensify in 2012—is the proliferation of malware targeting mobile devices.

Smartphones: the mobile malware threat

- Nearly 40% of large businesses now consider smartphones the device type posing the largest security threat.
- Malware targeting the Android operating system has increased 400%.
- 85% of smartphone users are not employing an antivirus solution to scan for malware.

Source: Juniper Networks[6]

CenturyLink™ Business

Until the last few years, the BlackBerry, with its robust native security features, was the de facto standard for corporate use. Today, your users may be just as likely to use Apple iPhones and Google OS-based Android devices—both for business and personal use.

"The majority of malware right now is being developed for Android-based mobile devices, with the second most popular being iOS devices," Brecl said, although Apple's more rigorous application approval process provides a bit more of a barrier. "But at the end of the day, large businesses don't care about the device itself. Even a $500 handset is immaterial compared with the value of the data stored on it if it gets in the wrong hands."

Protecting the data users access, store and share via mobile devices requires a combination of security solutions and user policies. Brecl recommends these four steps to protect data on mobile devices:

1. Tightly control what can be installed on mobile devices.
2. Install anti-virus and anti-spam on every device.
3. Detect and prevent installation of known malware.
4. Protect data on lost or stolen devices:
    - Enforce use of security PINs to control access.
    - Encrypt sensitive or proprietary data.
    - Use management capabilities to "remote wipe" data.

Social media: preying on trust

Social media has evolved to become a vital part of your business toolkit. Sure, employees are checking Facebook on their lunch break, but they're also using social tools to answer customer support calls, collaborate with colleagues and partners, and seek user input for new product innovations.

- 60% of employees use social media for personal reasons at least 30 minutes per day.
- 42% spend that much time on social media for business purposes.
- 52% of organizations experienced an increase in malware attacks as a result of employees' use of social media.
- 29% say they have the necessary security controls in place to mitigate or reduce the risk posed by social media used in the workforce.

Source: Ponemon Institute[5]

In addition to external social networks, your company's employees may share links on internal platforms such as Salesforce Chatter or an instant messaging application. "If I send you a link, you're going to click on it because it's from me—someone you trust. In the case of social networks, the bad guys count on being able to compromise someone's account and then utilize that trust to get you to click," Brecl said.

Even if a link really does come from a trusted friend or colleague, it doesn't mean the content is safe. In fact, it's estimated that about 80% of websites infected with malicious code are actually legitimate sites. That's why it's important to protect your network with Web content filtering, which enables you to limit user access to certain websites, either because they violate company policies or because malware has been detected. "Nothing is 100% fool-proof," Brecl said. "But it's better than just trusting blindly."

Cloud services: securing the virtualized frontier

As you consider moving business-critical applications to the cloud, security is bound to be top of mind. Although it trails other concerns, such as device theft, mobility and IT consumerization, only 40% of business and technology leaders in a recent IDG survey[7] are "extremely or very confident that their security infrastructure is prepared to protect data in the cloud."

According to the IDG report, preventing data leaks is the top cloud concern, followed by managing access to data and detecting and preventing intrusion.

Visibility into your data is essential. "In a corporate environment where you could walk down and touch your server, you had the tools to provide a great deal of visibility," Brecl said. "As you move into the cloud environment, the need for that visibility does not go away."

As companies like yours balance cloud security issues with the potential business benefits, one approach is a hybrid

CenturyLink™ Business

cloud solution. IDG notes that this "best-of-both-worlds" approach enables you to maximize the advantages of managed security services while maintaining control over your critical data protection strategy.

A secure strategy for 2012

Whether it's addressing mobility, social media or the cloud, Brecl advises a three-pronged approach for your 2012 security strategy.

1. **Technology:** Intensified security around mobile devices is critical as they face increasing exposure to threats.
2. **Policy:** Do your employees clearly know what is allowed and not allowed? Can they recognize suspicious links and content?
3. **Risk assessment:**
    - What is critical to your business?
    - How are you going to protect it?
    - How will you prevent downtime?
    - How will you get back up and running quickly?

Ultimately, Brecl said your 2012 security strategy must address both the technical and human vulnerabilities. "The people aspect is huge, because no technology alone can stop it."

Essential Questions for Cloud Security

- Where does your data actually reside?
- How well is your data protected?
- Is encryption in place?
- Are you in a shared environment or is it dedicated to you?
- If shared, what measures are in place to prevent cross-contamination?
- What are your logging capabilities?
- Do other systems that ensure compliance have access to the same information they did when servers were local?
- Are security information and event management services (SIEM) in place?
- Can you still analyze and react to those events in the same way you did before?

1. Forrester Research, Inc., *Sneak Peek At 2012 For Tech Marketers And Strategists*, December 3, 2010
2. *McAfee Q1 Threats Report Reveals Surge in Malware and Drop in SPAM*, McAfee, June 1, 2011
3. *Malware Surges 26% in 2011—report from PandaLabs*, InformationWeek, April 7, 2011
4. *Time to Embrace Employee-Owned Smartphones?*, Olafur Ingthorsson, Data Center Knowledge, July 26, 2011
5. *Global Survey on Social Media Risks, Survey of IT & IT Security Practitioners*, Ponemon Institute Research Report, Ponemon Institute, 2011
6. *Malicious Mobile Threats Report*, Juniper Networks, 2011
7. *Reaching for the Cloud*, IDG Research, Dec 2010

CenturyLink™
Business