CYBER SECURITY

Leading companies adopt new security tools

Warwick Ashford
Friday 01 February 2013 15:48

The actual number of cyber attacks on businesses is probably five times greater than the number being reported, according to Eddie Schwartz, chief information security officer at RSA.

“Only a few security firms understand how to detect and respond to attacks; most have got some catching up to do,” he said in a panel discussion at the Kaspersky Cyber Security Summit 2013 in New York.

Typically the biggest, most well-resourced companies are the ones thinking about how to evolve their products and services to meet new and emerging threats, he said.

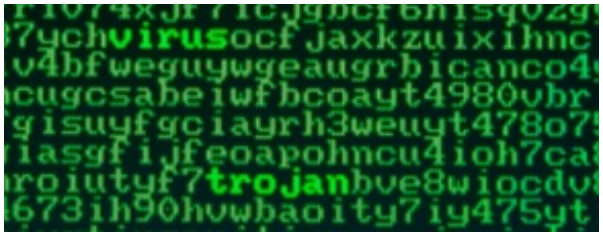
While attacks against corporates are

Latest News

- Ofcom launches consultation on liberalising 4G spectrum
- Datacentre boom will push demand for energy-efficient UPSs in Europe
- Don’t make big data stand alone, warns Gartner
- Claranet cloud powers Channel 5's Big Brother
- Government reviews data security rules to widen device clearance

MORE NEWS

Hot Topics



definitely increasing, not all corporates are standing still in their defence strategies, said Andy Steingruebl, senior manager, customer and ecosystem security at PayPal.

“Leading companies are upping their security, they are using the most up-to-date security tools,” he said, pointing out that a growing number of these tools are becoming available as part of standard IT services.

New technologies introduce new threats

At the same time, however, many companies are still struggling to come to grips with the security vulnerabilities presented by each new technology, said Adrian Stone, director security response for Research in Motion (RIM).

In terms of security evolution, RIM’s newly released mobile security offerings are designed to be as flexible, transparent and easy to manage as possible to make them attractive to users and administrators alike, he said.

For RSA, the security division of EMC, the strategy is to help organisations deal with new challenges such as maintaining control and visibility of their cloud computing environments.

Governance, risk and compliance in the cloud is an important area of innovation for RSA, said Schwartz.

Core to PayPal’s security strategy is tight control, which is derived from the firm’s ability to do almost everything itself and be transparent about all the data it collects and how that data is used, said Steingruebl.

A key strategy for Kaspersky in developing new products and services is to increase the cost of exploiting vulnerabilities for would-be attackers, said Costin Raiu, director of global research at Kaspersky Lab.

As part of increasing the cost to cyber criminals, Kaspersky Lab is working with

- Bett Show 2013
- Guide to mobile business intelligence
- Consumer Electronics Show 2013 coverage
- 2012: A review of the year
- Supplier profile: TCS

SEE MORE HOT TOPICS

Latest Blog Posts

- Computer Weekly Editor's Blog: Software is your salesperson - how to avoid agile annihilation
- Open Source Insider: Can open source save STEM (Science-Technology-Engineering-Mathematics) graduate figures?
- Inspect-a-Gadget: BlackBerry 10 hijacks your iOS and Android device thanks to Blippar
- Inside Outsourcing: Inside Outsourcing interview: Infosys trailblazer on iGate and the arrival of outcome based service
- Computer Weekly Data Bank: Telecom Services Spend - Information Services Companies

several software suppliers, such as Adobe and Microsoft, as well as law makers and law enforcement officers, he said.

Success can be measured by looking at the growing number of arrests being made and the reduction in financial losses through banking Trojans. “Any reduction is a good outcome,” said Raiu.

Advanced threats call for security review

However, PayPal's Steingruebl called for additional metrics such as those available for other forms of crime. Most other crimes are tracked closely from one year to the next, but not yet for cyber crime, he said.

A lack of historical data is also a problem when it comes to trying to explaining the business value of security and having discussions with the business around return on security investment, said Schwartz.

Now would be a good time for many businesses to review the way they invest in security, he said, with most companies putting 80% of investments in operations and management.

“Instead they should be investing to support their business objectives and to detect and deter attackers as well as defending their data,” he said.

RIM’s Adrian Stone also recommended that organisations think more carefully about the software they use and develop.

“They need to focus on secure development processes for internally developed software and invest more in application security testing for all software, including commercial products,” he said.

READ MORE ABOUT ADVANCED PERSISTENT THREATS (APTS)

- AT&T takes APTs seriously
- Conducting APT detection when Elirks, other backdoors hide traffic
- APTs: Are they really a concern for all businesses?
- Half of UK networks vulnerable to APTs
- Hardening the network against targeted APT attacks
- Surviving cyber war: Preparing for APTs, Stuxnet malware-style attacks
- Boost advanced persistent threat (APT) security levels in six steps
- Ranum chat: APT attacks and malware evolution

SEE ALL COMPUTER WEEKLY BLOGS

According to Stone, a sound security development lifecycle (SDL) should be all-encompassing, involving all parts of the business and including incident response as well as vulnerability management.

- Advanced persistent threat (APT) defense; best practices

Enterprise architecture is another important consideration that can be used to reduce risk, said PayPal's Andy Steingruebl.

"Simply ensuring that no credit card data is ever stored within company IT systems can dramatically reduce risk and regulatory compliance obligations," he said.

Identify weak spots in business processes

Similarly organisations should rethink all their business processes and not do anything that can be outsourced to someone else with greater expertise in that area, including disaster recovery, said Steingruebl.

In the wake of news that two major US newspapers have been infiltrated by Chinese hackers, security experts have said the incidents underline the fact that traditional, often perimeter-based security defences are increasingly ineffective against targeted, persistent attacks.

> **It is no longer a matter of if attackers get in, but when**
>
> Martin Roesch, Sourcefire

Targeted attacks, commonly termed advanced persistent threats (APTs), not only penetrate defences, but also spread laterally and establish a long-term foothold in the network, said Jason Steer, European product manager and architect for security firm FireEye.

"The cyber economic advantage is therefore with offence – as the cost to launch an attack is often negligible, while the cost to defend against every possible attack is high," he said.

With the odds stacked against businesses, Steer said it is vital that companies take into account the targeted nature of today's threat, particularly those firms with

intellectual property and other highly sensitive assets to protect.

“As we can see, hackers of varying levels have become very adept at overcoming traditional forms of security,” he said.

According to Steer, a comprehensive strategy that includes both traditional and proactive signature-less solutions is the only way to truly bolster defences against attackers.

Security firm Sourcefire said “retrospective” security capabilities may have mitigated the risk.

Retrospective alerting highlights files previously seen and thought to be safe but now, according to the latest threat information and analysis, are identified as malicious.

“This incident is the latest example of how attackers and their tools have advanced to evade traditional defences,” said Martin Roesch, founder and interim CEO of Sourcefire.

“The reality is that it’s no longer a matter of if attackers get in, but when. Point-in-time security that only has one shot to determine if a file is malware does not work by itself,” he said.

A new model that also collects telemetry for continual analysis of what is happening in an IT environment is needed to determine scope, contain and ultimately remediate the malware automatically, said Roesch.

Related Topics: Hackers and cybercrime prevention, IT for utilities and energy, Data breach incident management and recovery, IT for consulting and business services, IT risk management, Application security and coding requirements, IT for transport and travel industry, IT for manufacturing, IT for charity organisations, IT for telecoms and internet organisations, Privacy and data protection, IT for leisure and hospitality industry, IT for small and medium-sized enterprises (SME), IT for government and public sector, IT suppliers, IT for retail and logistics, Antivirus,

firewall and IDS products, Business continuity planning, IT for media and entertainment industry, IT for financial services, VIEW ALL TOPICS

Email Alerts

Register now to receive ComputerWeekly.com IT-related news, guides and more, delivered to your inbox.

Email Address GO

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy

Read More

RELATED CONTENT FROM COMPUTERWEEKLY.COM

- More firms targeted by advanced persistent threats, study finds
- AT&T takes APTs seriously
- Confusion over APT attacks leads to misguided security effort
- RSA 2011: RSA, EMC and VMWare advise on defending against advanced persistent threats
- RSA hit by advanced persistent threat attacks

RELATED CONTENT FROM THE TECHTARGET NETWORK

- Genpact boosts security management with SIEM tool
- Clearing networking and security hurdles of private cloud adoption
- Taking the lead in an Agile enterprise
- Midmarket companies take the lead on cloud computing adoption
- Midmarket companies take the lead on cloud computing adoption

DISQUS

// Commenting policy

BACK TO TOP

More from Related TechTarget Sites

CIO

SECURITY

NETWORKING

DATA CENTER

DATA MANAGEMENT

SearchCIO

TechTarget

Mobile application development: Fast, furious -- and flawed?

Mobile application development is a competitive race, so is it more important to get mobile apps out the door fast? Or out feature-rich and flawless?

Is the 'cloud center' the new data center?

Is 'cloud center' a more accurate term than 'data center' in today's IT organizations? In our inaugural tweet jam, our Twitter followers weighed in.

Information security breach at 'The New York Times' is one scary story

In this week's Searchlight: a chilling information security breach at 'The New York Times', plus how 'big data' will save us all. Or maybe it won't.