Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Fax: +44 (0)1865 843973
Web: www.networksecuritynewsletter.com

Publisher: Greg Valero
E-mail: g.valero@elsevier.com

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

International Editoral Advisory Board:
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1112 for all European countries & Iran
US$1244 for all countries except Europe and Japan
¥147 525 for Japan
(Prices valid until 31 December 2011)
To subscribe send payment to the address above.
Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971
Email: commsales@elsevier.com,
or via www.networksecuritynewsletter.com
Subscriptions run for 12 months, from the date payment is received. Periodicals postage is paid at Rahway, NJ 07065, USA. Postmaster send all USA address corrections to: Network Security, 365 Blair Road, Avenel, NJ 07001, USA

Pre-press/Printed by
Mayfield Press (Oxford) Limited

...Continued from front page

The 2011 (ISC)^2 Global Information Security Workforce Study (GISWS), conducted by industry analysts Frost & Sullivan, suggests that although information security practitioners are aware that new skills are needed for the move to the cloud, the areas of most concern to them are the very ones that tend to be delegated to the cloud service supplier.

Of the 7,500 (ISC)^2 certified professionals polled for the survey, nearly three-quarters admitted that they would need to acquire new skills to properly and securely manage the move to cloud-based architectures. When asked what these skills were, 93% said they would need a detailed understanding of cloud computing, and 81% wanted enhanced technical knowledge. Only half put contract negotiation abilities in their top three requirements.

"It is surprising to see such an emphasis on technology and detail when we are looking at a trend involving outsourcing the management of it," said Robert Ayoub, Frost & Sullivan's lead analyst on the study. "Professionals, the majority of whom have a technical background, appear to be focusing on the familiar. The instinct to develop skills for the new operational dynamic introduced by cloud computing may still be elusive for many."

More than half of the organisations for which these professionals work are already using cloud services to some degree. Some 16% are using public cloud services and 42% are making use of Software as a Service (SaaS). But many still have security concerns, with data leaks worrying 85% of the people surveyed. Some 68% rate weak system or application access controls as a major concern, cyber-attacks are an issue for 65% and disruption to the service keeps 62% of them awake at night.

"The concern over risks to data suggests that we as a profession recognise the need to master our understanding of how data is used and valued by the business and its customers," said John Colley, managing director EMEA, (ISC)^2. "This goes beyond understanding the technology and detail of the systems. IT is a tool of the business, and it is the business itself, its processes and the information it uses that must be understood."

Very few of the respondents were worried about their jobs. Less than 10% thought that cloud computing was going to have a negative effect on the demand for information security professionals, and about half thought that demand would increase.

The full report is due out in February.

Two other security organisations – ISACA and the Information Security Forum (ISF) – have joined forces with (ISC)^2 to promote good practice in information security. They have defined a set of 12 principles that they believe will help information security professionals in their task of supporting corporate governance, regulatory compliance and risk assessment.

"There are other standards and frameworks around like SOGP, COBIT and ISO27002, which are all aimed at organisations, but we were clear that we wanted these principles to be unique, practical and more like a code of conduct for individuals to adopt," said Jason Creasey, global alliances leader, ISF. "These principles, which ISF has spearheaded over the past 12 months, will help align security more closely with essential business activities and enable security practitioners to create a security-positive environment and better manage information risks."

The guidelines are available from all three organisations' websites: the ISF has them here: <http://bit.ly/201101principles>.

Wifi security cracked

It may be necessary to regard all wifi connections as potentially insecure after a German security researcher demonstrated an ability to crack WPA-PSK passwords.

Brute-forcing WPA-PSK passwords using dictionary attacks has long been considered an unlikely attack vector because of the computing resources required. But Thomas Roth wrote his software to use Amazon's EC2 cloud-based computing resources, and was able

Continued on page 20...

...Continued from page 2

to crack passwords for as little as $1.68.

The method builds on work carried out by Moxie Marlinspike and his WPACracker service, which uses a 400 CPU cluster on the Amazon cloud. Roth took this further using Amazon's 'cluster GPU instances' infrastructure.

Roth had previously carried out research using the Amazon service to brute-force SHA-1 hashes. As a result of the new Amazon service, he said, it's now easy for anyone to create a 100-node (or more) cluster and distribute the task of cracking passwords. It turns out that the job of cracking hashes is perfectly suited to mass parallelisation, he added.

With this architecture, he believes it's possible to try up to 400,000 passwords a second. He was able to break into a WPA-PSK protected network in around 20 minutes and believes this could be reduced to as little as six.

Roth's blog is at: <http://stacksmashing.net>.

Passwords not up to the task

The humble password has had its day and is no longer up to the task of securing access to modern infrastructures and technologies, says a report from Forrester Consulting, commissioned by Symantec.

Reliance on the traditional ID/password combination is leaving organisations open to unauthorised access by hackers and cyber-criminals and simply isn't capable of dealing with the modern environment of cloud computing, collaboration tools and mobile devices such as smartphones. All of these project the IT environment well beyond traditional corporate boundaries.

While malware still presents a great threat to corporate security, the use of stolen passwords is becoming an increasing menace, the report finds. Organisations have responded with ever more cumbersome and error-prone password policies. More complex passwords, shorter expiration deadlines and the use of multiple passwords are making life difficult for end users and placing heavy loads on help desks: password issues account for 30-50% of help desk calls.

Corporate networks are also vulnerable because of a lack of strong authentication when communicating with the networks of partners. Symantec's report found that 67% of organisations do not require strong authentication when a partner's network connect to theirs.

The report goes on to make a number of recommendations. Top of the list is the suggestion that organisations reassess the use of strong authentication and two-factor authentication in particular.

"The IT landscape is changing so dramatically and so rapidly that one in four organisations is requiring users to remember six or more passwords to access corporate networks and applications," said Atri Chatterjee, vice-president of user authentication at Symantec. "That approach to authentication is collapsing under its own weight. Today's strong authentication offers a way to easily manage and control access to enterprise applications and networks via both computers and mobile devices."

Data leaks result from malicious intent

The majority of data leaks are the result of deliberate and malicious acts by hackers and insiders rather than stemming from accidents or incompetence. That's the verdict of an analysis by the Identity Theft Resource Center (ITRC) in the US.

The organisation recorded at least 662 data breaches in 2010, exposing more than 16 million records. Hacking attacks accounted for 17.1% of these – more than any other single cause – and theft by insiders added another 15.4%. Accidental exposure via the web resulted in 11% of the leaks and another 16.6% were due to moving data unprotected on portable media.

The true scale of the problem is hard to define, however, as nearly half of the organisations that suffered data breaches failed to report how many records were involved. In fact, some don't report data breaches at all. Some US states have data breach notification laws, but enforcement is patchy.

EVENTS CALENDAR

15 February 2011
Information Assurance in the Age of Austerity
London, England
Website: www.ia-conference.com

22 – 24 February 2011
ICCNSS 2011: International Conference on Computer Networks and Systems Security
Penang, Malaysia
Website: www.waset.org/conferences/2011/penang/iccnss/

25 February – 3 March 2011
SANS Phoenix 2011
Phoenix, US
Website: www.sans.org/phoenix-2011

28 February – 4 March 2011
Financial Cryptography and Data Security '11
St Lucia
Website: ifca.ai/fc11/program.html

15 – 18 March 2011
Blackhat Europe 2011
Barcelona, Spain
Website: www.blackhat.com

27 March – 4 April 2011
SANS 2011
Florida, US
Website: www.sans.org/sans-2011/

19 – 21 April 2011
Infosecurity Europe 2011
London, UK
Website: www.infosec.co.uk

16 – 19 May 2011
IFSEC
Birmingham, UK
Website: www.ifsec.co.uk

30 July – 4 Aug 2011
Blackhat 2011
Las Vegas, Nevada, US
Website: www.blackhat.com