[IN]SECURE

infosecurity EUROPE

29 April - 01 May 2014 | Earls Court | London | UK

345 EXHIBITORS
15,000 VISITORS

QUALYS®

Welcome to (IN)SECURE Magazine special issue: Infosecurity Europe 2014

At this year's Infosecurity Europe conference and exhibition, senior figures from both government and industry have called for greater collaboration on how security intelligence is shared, in order to protect against cyber-attacks and ensure that security insight spreads beyond IT teams to affect boardroom decisions.

The show, which attracted more than 15,000 unique industry professionals from 73 countries across the three days, had a massive show floor featuring 345 exhibitors from 24 countries. Presented in this issue are some of the most interesting news and companies we've seen at the show.

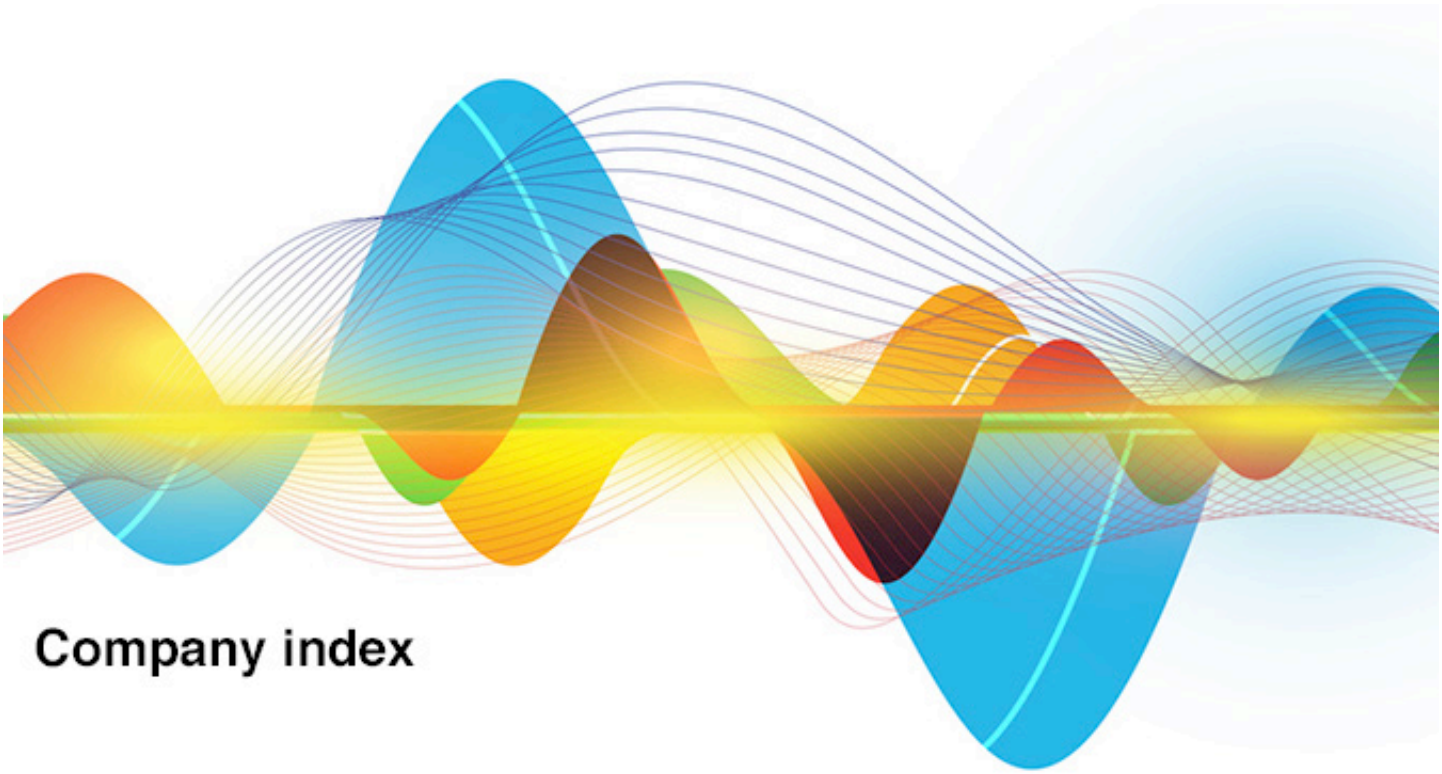
Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@net-security.org
News: **Zeljka Zorz**, Managing Editor - zzorz@net-security.org
Marketing: **Berislav Kucan**, Director of Operations - bkucan@net-security.org

Distribution



Company index

Below is an index of companies featured in this issue, along with the page number.

CoSoSys updates Endpoint Protector 4

CoSoSys updated the Endpoint Protector 4 platform, which provides IT administrators with improved Content Aware Protection policies on the management side, as well as the reporting side.

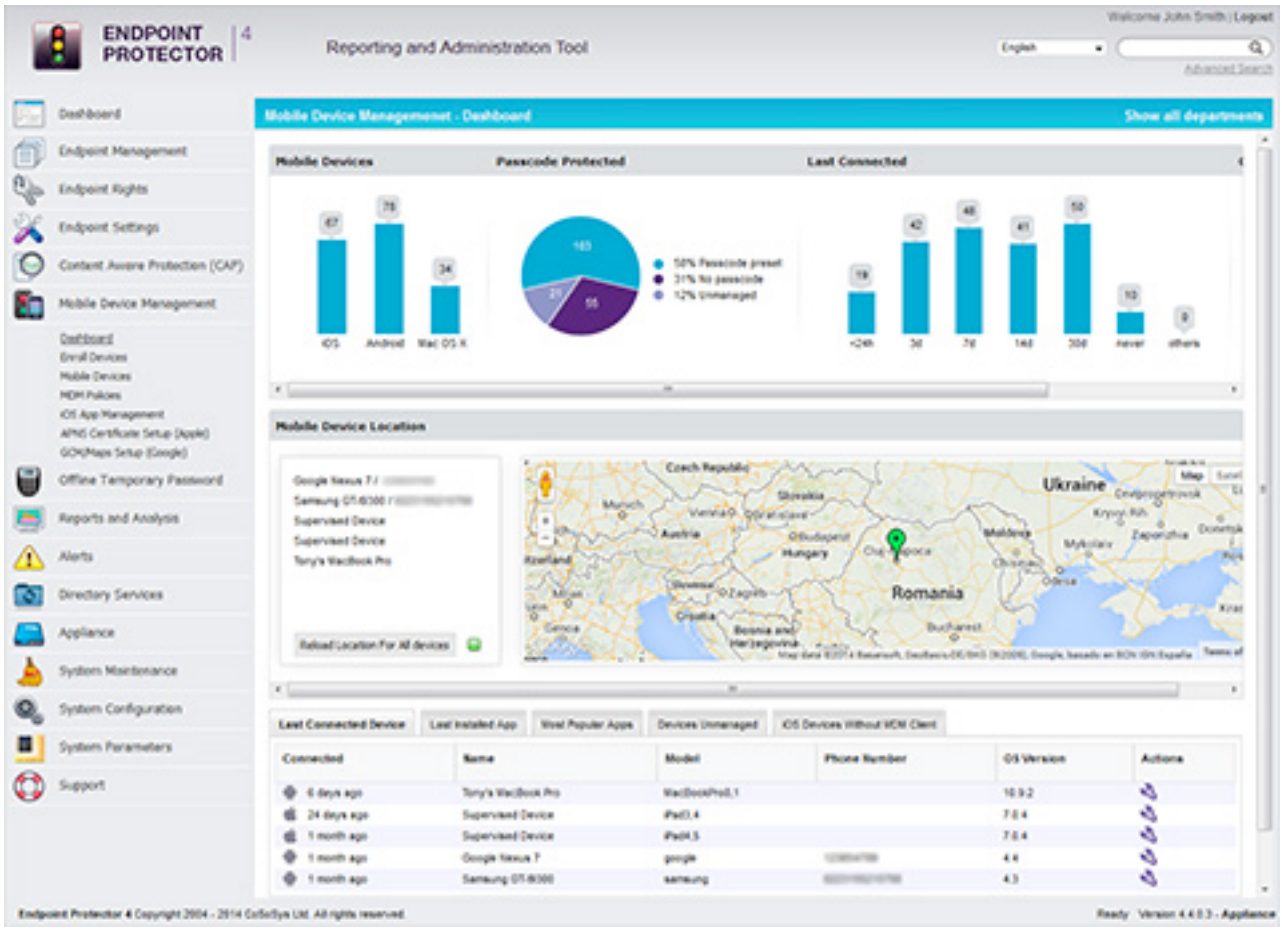
The new version also includes enhancements for the Mobile Device Management (MDM) module that will allow them to perform more advanced actions to better secure mobile devices and computers across multiple operating systems including OS X, iOS and Android.

Roman Foeckl, CEO and Founder of CoSoSys, comments: “Demand for IT services that can incorporate Macs onto their networks is at an all time high, and we are proud to offer not only the first Enforced Encryption for removable devices on Macs solution and the first Content Aware Protection solution for Macs, but now we are taking full advantage of the OS X offerings to make sure we are addressing data loss from all perspectives.”

For the Mobile Device Management module, updates include expanding support for Macs in the Endpoint Protector 4 platform to help businesses secure data on all endpoints. Macs are enrolled the same way as iOS devices are and features like Passcode Setting, File Vault 2 Full Disk Encryption, control of VPN, Mail and WiFi, as well as other features are available now for MacBooks and iMacs.

Endpoint Protector Version 4.4.0.3 brings updates for the Android platform as well. Controlling Android devices can be done at a higher level, with more sophisticated functionalities. Mobile Application Management (MAM) is another key addition that has been requested by a significant number of customers and partners. Pushing apps to Android mobile devices is a priority for an increased number of companies, due to a better control of what employees use for work purposes derived from this feature.

Other actions that can be performed with this release include enabling encryption, activating/deactivating Wi-Fi, Bluetooth and camera, visualizing/editing calendar events.




CYBERARK


Trusted Applications
Mobility Empowerment


CONTINUOUS SECURITY
Find vulnerabilities first, match every threat, anticipate every move
Continuous Security in a Unified Cloud Platform:
ASSET DISCOVERY
NETWORK SECURITY
COMPLIANCE MONITORING
WEB APP SECURITY
THREAT PROTECTION
QUALYS


dimension data

Security pros and government failing to collaborate

Infosecurity Europe released a new report that provides a snapshot of the industry landscape and the challenges it is currently facing.

Having surveyed 1,149 information security professionals from across the world, the report highlights the increasing importance of information security to business strategy – from the effect of Edward Snowden's NSA leaks and the impact of big data, to the demand for boardroom education and the need to develop a long-term strategy to combat evolving threats.

Historically viewed as an obstacle to business, information security is gradually being recognized as a business enabler.

The report also reveals that more effective collaboration between government and the information security industry is crucial to protecting organizations from future cyber threats. Additionally, more work needs to be done to strengthen government's position as a source of information on potential threats: only 4.8% of information security professionals selected the government as their most trusted source for intelligence.

"This is something that needs to be addressed urgently," said Brian Honan, Founder & CEO, BH Consulting, who was a speaker at Infosecurity Europe 2014. "Without better collaboration between industry and governments we are at a disadvantage against our adversaries. As threats and the capabilities of those looking to breach our systems evolve we need to jointly respond better in how we proactively deal with the threat. We need industry and government to work together in ensuring a strategic approach is taken to enabling companies and citizens to be more aware of the threats to their data, to educate them in how to deal with the threat, and finally how to work together at national and international level to tackle the threats we face."

Data security is being pushed up the agenda according to the survey, possibly catalyzed by the Snowden revelations in June last year. The NSA exposé has triggered action, with 58.6% believing the Snowden affair has been positive in making their business understand potential threats. Despite this, it's clear boardroom recognition needs to improve, as 46.7% feel it has not been easier to make their business understand the challenges they face as a result of the leaks.

While, on the whole, the industry is coping with the deluge of data they receive, 30.5% of information security professionals feel their organization isn't able to make effective strategic decisions based on that data. Considering the majority have seen this volume of data increase over the past 12 months, adopting a future-proof approach to information security is going to become increasingly important. Worryingly, 47.4% believe the industry has a short-termist approach, lurching from one threat to another.

Widespread uncertainty about cloud security

More and more organizations are transferring sensitive or confidential information to public cloud services even though more than a third expect a negative impact on security posture. In response, the use of encryption is increasing but more than half of respondents still admit their sensitive data goes unprotected when it is stored in the cloud, despite data security topping the global news agenda.

Released at Infosecurity Europe 2014, the independent global study of more than 4,000 organizations conducted by the Ponemon Institute reveals differing opinions over who is responsible for security in the cloud – the cloud provider, or the cloud consumer and how best to protect the sensitive data that is sent there.

Cloud security is here to stay: The use of the cloud for processing and storing sensitive data seems inevitable. More than half of all respondents say their organization already transfers sensitive or confidential data to the cloud and only 11 percent say that their organization has no plans to use the cloud for sensitive operations, down from 19 percent only two years ago.

Cloud confidence is on the up, but at what cost? Although nearly half of respondents believe that their use of the cloud has had no impact on their overall security posture, those that believe it has had a negative effect (34 percent) on their security posture outnumbered those that experienced a positive effect (17 percent) by a factor of two to one.

Where does the security buck stop? The perceived responsibility for protecting sensitive data in the cloud is very dependent on the type of cloud service in question. In SaaS environments more than half of respondents see the cloud provider as being primarily responsible for security. In contrast, nearly half of IaaS/PaaS users view security as a shared responsibility between the user and cloud provider.

Visibility improves but gaps remain: The good news is that visibility into the security practices of cloud providers is increasing with 35 percent of respondents considering themselves knowledgeable about the security practices of their cloud providers compared with 29 percent only two years ago. But, half of SaaS users still claim to have no knowledge of what steps their providers are taking to secure their sensitive data.

Encryption usage increases but data still exposed: The use of encryption to protect sensitive or confidential data stored in the cloud (data at rest) appears to be increasing. For SaaS users we see an increase from 32 percent in 2011 to 39 percent in 2013 and for IaaS/PaaS users respondents report an increase from 17 percent to 26 percent over the same period, but still, more than half of respondents report that their sensitive data is in the clear and therefore readable when stored in the cloud.

Treading a line between trust and control: There is currently an almost equal division in terms of how stored data is encrypted while in the cloud. Of those respondents that encrypt stored data just over half apply encryption directly within in the cloud with just over 40 percent elect to encrypt the data before it is sent to the cloud.

Who holds the key? When it comes to key management there is a clear recognition of the importance of retaining ownership of encryption keys with 34 percent of respondents reporting that their own organization is in control of encryption keys when data is encrypted in the cloud. Only 18 percent of respondents report that the cloud provider has full control over keys.

Standards enable trust in a shared environment: The need to share keys between organizations and the cloud highlights the growing interest in key management standards – in particular OASIS Key Management Interoperability Protocol (KMIP) – where 54 percent of respondents identify cloud based applications and storage encryption as the area to be most impacted by the adoption of the KMIP standard.


Centrify
CINEMA
Centrify
Centrify
discuss emerging security threats over a coffee
zscaler
divide
Acronis
MobileIron
MobileIron
Device Control
Data Loss Prevention (DLP)
Windows / Mac OS X
Device Control
Windows / Mac OS X / Linux
Mobile Device Management (MDM)
iOS / Android
ENDPOINT PROTECTOR
EU
EndpointProtector.com

Spike in DDoS attack size driven by NTP misuse

The beginning of 2014 saw 1.5 times the number of attacks over 20GB/sec, compared to the rest of 2013, according to stats released by Arbor Networks.

The company released global DDoS attack data derived from its ATLAS threat monitoring infrastructure, which shows an unprecedented spike in volumetric attacks, driven by the proliferation of NTP reflection/amplification attacks.

NTP is a UDP-based protocol used to synchronize clocks over a computer network. Any UDP-based service including DNS, SNMP, NTP, chargen, and RADIUS is a potential vector for DDoS attacks because the protocol is connectionless and source IP addresses can be spoofed by attackers who have control of compromised or 'botted' hosts residing on networks which have not implemented basic anti-spoofing measures.

NTP is popular due to its high amplification ratio of approximately 1000x. Furthermore, attacks tools are becoming readily available, making these attacks easy to execute.

NTP attacks highlights

· Average NTP traffic globally in November 2013 was 1.29 GB/sec, by February 2014 it was 351.64 GB/sec
· NTP was used in 14% of DDoS events overall but 56% of events over 10 GB/sec and 84.7% of events over 100 GB/sec
· US, France and Australia were the most common targets overall
· US and France were the most common targets of large attacks.

"Arbor has been monitoring and mitigating DDoS attacks since 2000. The spike in the size and frequency of large attacks so far in 2014 has been unprecedented," said Arbor Networks Director of Solutions Architects Darren Anstee. "These attacks have become so large, they pose a very serious threat to Internet infrastructure, from the ISP to the enterprise."

Data encryption for secure communications

IGUANA Security launched the latest addition to its family of Critical National Infrastructure (CNI) solutions.

IGUANAGreen is a commercial encryption solution designed to encrypt and protect sensitive data at the highest level, enabling secure communications across public IP networks. It's part of the IGUANA Security family of solutions, designed for the protection of critical networks and data assets, defending against the proliferation of complex cyber attacks.

IGUANAGreen, a flexible voice and data solution, and IGUANAGreen for Enterprise, a high-speed, low-latency device, offer hardware-based protection that results in an exceptionally small attack surface. This increases resilience to network attacks and malware, providing the most dependable protection for critical IT infrastructure.

Code analysis and app security testing simplified

Quotium released Seeker Enterprise 3.0, whose technology correlates application behavior with simulated hacker's attacks to pinpoint vulnerable code.

Seeker is the run-time code & data analysis application security testing solution for the SDLC. It assists in vulnerability management by accurately demonstrating risks to business critical data. It can be fully automated and is very suitable for Agile and continuous integration environments.

Delivering an application security testing automation process in the development lifecycle, it allows organizations to secure every build, every release and every application without requiring manpower overhead or specific security knowledge.

Seeker's capabilities that allow organizations to handle software cyber threats in development environments. The new dashboards allow executives and managers to view their overall organizational security status, see which systems pose the most threat, which compliance requirements are met and which aren't.

Data Loss Prevention | Device Control
Mobile Device Management | Encryption

ENDPOINT PROTECTOR | by CoSoSys

Easy to use, trusted around the globe and used by millions

www.EndpointProtector.com

Cyber intelligence services reveal sensitive data firms are leaking online

Digital Shadows has launched SearchLight – a suite of managed cyber intelligence services designed to reveal sensitive data companies are leaking online and which hostile groups are targeting them.

Threat SearchLight uses data mining and other analytical techniques to continuously monitor hostile groups and their operations to identify the "who, what, where, when and how" of a targeted attack.

It draws on over 80 million information sources in 26 languages across the globe. Sources include social networking sites, blogs, forums, cyber criminal sites, chatrooms, search engines, file sharing sites and other places within the "dark web".

Defacement mitigator for cybersecurity protection

Foresight released Defacement Mitigator, the first cloud-based web security solution that provides full defacement mitigation and protection to government, academic, religious, financial services, and other organizations targeted by cyber hacktivists.

Defacement Mitigator is available as a managed service (SaaS) and sold as a stand-alone product or as part of Foresight's cloud-based web security platform. Pricing is based on the number of domains and user traffic.

A hybrid approach to web app security assessment

High-Tech Bridge introduced its hybrid web application security assessment SaaS, ImmuniWeb for the first time ever to visitors at Infosecurity Europe 2014.

The service, which was developed in-house by High-Tech Bridge, is now in open Beta. The ImmuniWeb security assessment is the first hybrid service that combines automated vulnerability scanning and manual penetration testing to allow companies to conduct a quick and efficient website security review and ensure that a website or web apps are secure.

Priced at $639 (or 461 Euros / £380), the service comprises 12 hours of manual penetration testing by High-Tech Bridge security auditors, combined with an automated scan by the company's proprietary vulnerability scanner.


WAS
Addressing the challenges
Too many to protect
• Discover and catalog all web applications on network
• Prioritize identification of high severity vulnerabilities
• Securely share vulnerability information
Need to reduce risk quickly
• Leverage automated scanning
• Focus on high severity
• Protect identified vulnerabilities with WAF
• Monitor for malware
Lack of integrated approach
• Leverage a platform to gain efficiencies
• Share information and combine defenses
QUALYS


L80
Spikes Security
SPIKES
SECURE YOUR BROWSER
PROTECT YOUR BUSINESS


QUARRi


corero
FIRST LINE OF DEFENSE


Good
NETWORKING BAR

Airbus Group debuts SCADA research project to mitigate ICS vulnerabilities

Airbus Group highlighted its range of technologies, services and a research project to help governments and industry deal with the increasingly complex and unpredictable nature of cyber attacks.

Debuting in the UK, details of a £1.2M SCADA research project will be disclosed, which is aiming to understand and mitigate the vulnerabilities in the industrial control systems that drive Critical National Infrastructures (CNI) such as gas, water, transportation networks and banking systems.

The three-year project is a collaboration between the Airbus Group Innovations research centre, the EADS Foundation Wales, three universities and the Welsh Government. A robotic arm production demonstration will highlight the potential weaknesses in industrial control systems and showcase some of the cyber security mechanisms that can be used to prevent potentially disastrous implications of a cyber attack on UK Critical National Infrastructure.

Advanced cybersecurity capabilities including the innovative Cyber Defence Centre services will also be an important part of the Airbus Defence and Space offering this year.

Most enterprises use cloud storage, but don't trust it completely

A global survey of 912 businesses reveals that although 83 percent of businesses surveyed back up some part of their data to the cloud, there is a strong reluctance to embrace the medium fully. In fact, 47 percent of respondents store less than half of their data in the cloud and 17 percent do not use cloud storage at all, the results of the survey revealed at Infosecurity Europe 2014.

Of the companies surveyed that are using a cloud storage solution, 69 percent consider the data they store there as sensitive. However, 16 percent of companies surveyed have experienced problems with their cloud provider.

Of these, 42 percent had found that the data held by their cloud provider was not secure. Meanwhile, 40 percent claimed that data held in the cloud had not been available when needed and over one-third (37 percent) said their cloud provider had actually lost their data.

Further, approximately 89 percent of the firms surveyed cited the security credentials of their cloud provider as important or very important. Respondents said that they are more than twice as likely (53 percent vs. 23 percent) to trust a security vendor than a storage vendor to keep their data safe in the cloud.

63% of orgs believe they can’t stop data theft

Websense released the first report of the Ponemon Institute survey, “Exposing the Cybersecurity Cracks: A Global Perspective,” which gives new insight into why cybercriminals have a foothold in the broader enterprise.

The new survey of nearly 5,000 global IT security professionals reveals a deficit in enterprise security systems, a disconnect in how confidential data is valued and limited visibility into cybercriminal activity.

Most respondents (69 percent) believe cybersecurity threats sometimes fall through the cracks of their companies’ existing security systems.

According to respondents, there is a gap between data breach perception and reality – specifically regarding the potential revenue loss to their business. 80 percent of respondents say their company’s leaders do not equate losing confidential data with a potential loss of revenue. This is in contrast to recent Ponemon Institute research, which indicates that data breaches have serious financial consequences for organizations.

The average cost per lost or stolen record due to a data breach is $188 and the average cost of an organizational data breach is $5.4 million.

The importance of visibility for today's complex networks

The complexity of modern enterprise networks is increasing due to a number of factors, and deeper levels of network visibility are necessary to aid in their management and troubleshooting, say the results of an Emulex study.

Of particular note, 69% of respondents stated that they expect the number of requests to capture network data (including metadata and packet-level data) to increase dramatically, driven by the needs of a variety of IT groups including network architecture, security, compliance, applications, and IT audit teams.

The survey polled 150 IT professionals from various industries, all from enterprises with 1,000 or more employees.

Sophos Cloud manages Windows, Mac and mobile devices

Sophos announced the latest version of Sophos Cloud, the company's cloud-based solution for small- and mid-sized organizations seeking a simpler approach to IT security that still provides world-class protection. The new version of Sophos Cloud is the only cloud-managed security service to manage Windows, Mac and mobile devices from a single console. It features user-based management, reporting and licensing; built-in web security to prevent user access to malicious and infected websites, and new policy-based Web Control features to enforce safe and productive web usage.

Sophos Cloud's new web features enable IT managers to easily set and enforce policies for enhanced security and compliance; user-based policies can be created once and rapidly deployed across multiple groups and platforms, and follow the users and their devices even when they are off the network.


SQUARED
AWAY
?
CISSP
SSCP
CSSLP
CCFP
HCISPP
www.isc2.org


dimension
data


ENERATION SECURITY - PROTECT YOUR
WatchGuard
INTRUSION PREVEN
CED PERSISTENT THR
YOD
EMAIL ENCRYP
APPLICATION CO
WIRELESS ACCESS
UTM


Talk to me
about
mobile
security


You can't hack
STEALTH


Check Point
SOFTWARE-DEFINED
PROTECTION
NTSC
COMODO
Check Point

London warbiking reveals worrying state of Wi-Fi security

Sophos highlighted the worrying state of wireless security when it sent security expert James Lyne and his computer-equipped bicycle onto the streets of London to test how safe homes, businesses, and even people on mobiles phones are from cyber criminals.

Lyne went warbiking across the city to track down insecure wireless networks and spotlight user behaviors that could be exploited by rogue hackers, and he discovered some alarming results: “Incredibly, conventional wireless network security is still a major concern, despite the security industry assuming such issues had been resolved years ago. Many would assume these methods are ‘old hat’ but it is still a very viable attack vector that demonstrates basic security best practice is not being adopted. ” says Lyne.

London was the latest stop on the “World of Warbiking” tour - a global research project targeting major cities across the globe. Conducted over two days around the streets of the capital, Lyne’s warbiking exercise revealed that of 81,743 networks surveyed, some 29.5 percent were using either the known-broken WEP algorithm, or no security encryption at all. A further 52 percent of networks were using WPA - a no longer recommended security algorithm.

CSA releases Software Defined Perimeter 1.0

The Cloud Security Alliance (CSA) released two key documents related to the CSA's Software Defined Perimeter (SDP), an initiative to create the next generation network security architecture.

As part of the updated framework, key concepts comprising the SDP, such as Single Packet Authorization and Mutual Transport Layer Security have undergone extensive review. Additionally, a number of CSA members, including some of the largest global companies, have SDP pilots in place.

IT security pros surprisingly cavalier about mobile security best practices

A flash poll conducted at Infosecurity Europe 2014 by Centrify has found that 94 per cent of IT security professionals use third party applications on their mobile devices for work, with 82 per cent using up to 10 apps.

“Applications are now at the heart of corporate IT and have become a vital part of how employees get the job done whilst either in the office or on the move. Removing access to applications isn't an option - in fact it would create more problems than it would solve," says Darren Gross, EMEA Director, Centrify. "But the risk for organizations is that the more cloud-based or mobile apps employees interact with, the more they create islands of identity that become harder for IT to track and manage."

“How do you access for thousands of employees across multiple devices and platforms? Let alone de-provision them when they leave the company. Identity and access can often be overlooked, but unless enterprises can find a unified way to securely identify individuals, they risk their business coming to a shuddering halt,” he added.

The poll also revealed that of the 169 people surveyed, 7 per cent of security professionals do not believe it is their responsibility to protect corporate information held on their personal device. A further 8 per cent do not have a password or PIN enabled on the mobile device that they use for work purposes, potentially exposing organizations to risk.

Surprisingly, despite repeated warnings about the risks posed by WiFi networks, 52 per cent of respondents said that they have accessed sensitive corporate information over insecure networks at locations such as a coffee shop or airport.

Gross concluded, "As the poll shows, the majority of employees are now leveraging more and more applications on their mobile devices. We are now seeing a greater need than ever for unified security identity across multiple devices and platforms."

The first Continuous Automated Incident Resolution (CAIR™) Platform, delivering comprehensive, real-time insight, analysis, response and resolution of data incidents.

ResolutionOne™ Platform

Cybersecurity

E-Discovery

Enterprise Investigations

AccessData®

Learn more at
http://accessdata.com/ResolutionOne-Platform