SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA

CYBER SENTINELS

VOLUME 03 | ISSUE 06 | **MAY 2017**

ENDING THE GAME OF THREATS

The recently announced partnership between Spire Solutions and Endgame beckons a new era in the continuous prevention and detection of zero days, ... 20

NATE FICK,
CEO, ENDGAME

STRATEGIC SECURITY PARTNER
GBM

KEEPING UP WITH THE CYBER THREAT LANDSCAPE

Let's face it, with everything becoming digital, cyber security is becoming a growing concern for organizations globally. In times of financial pressure or instability, security is often seen as a supporting function or an overhead cost to business. Questions such as when and how come up when it comes to safeguarding our organisations from potentially lethal cyber-attacks. With the region becoming a hub for many industries and seeing an increasing consolidation of wealth and assets, it's guaranteed to attract malicious players."

BY: AISHA NIZAMUDDIN KHAN <AISHA@GECMEDIAGROUP.COM>

Enterprises are transforming their security spending strategy in 2017, shifting from prevention-only approaches to focus more on detection and response, according to Gartner, Inc. Worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6 percent over 2016 and to top $113 billion by 2020. Spending on enhancing detection and response capabilities is expected to be a key priority for security buyers through 2020. The Internet of things has become the Internet of threats for security companies. Cyber security is the hot topic in the defence industry, with sales on the rise. Defence firms are expanding into this area as its the top priority for many governments around the world. Most importantly defence budgets have increased in the Middle East to include cyber security as cyber-attacks targeted national energy companies in the Middle East last year. Hence, IT security spending in the MENA region is estimated to reach $155.8 billion in 2017, a 2.4% increase from 2016. Verticals driving this spending will be media, communications, banking and securities and manufacturing.

"Talos' core objective is to provide verifiable and customizable defensive technologies and techniques that help customers quickly protect assets from the cloud to core."

-WARREN MERCER,
SECURITY RESEARCHER, CISCO TALOS

"FireEye provides unmatched threat intelligence strategies allowing organizations to mitigate risk, bolster incident response and enhance overall security."

-JENS CHRISTIAN HOY MONRAD,
SENIOR INTELLIGENCE ANALYST, FIREEYE.

CTIB IN THE MIDDLE EAST

The Middle East is dominated by major financial, energy and telecoms businesses, all of whom are vulnerable to cyber exploitation and attack. The UAE is currently the target of five percent of the world's cyber-attacks, with the financial services industry the worst affected. In this growing digital world, data privacy and its protection is most crucial for businesses. "As the threat has grown we have seen more investment by regional businesses to protect themselves from cyber-attack, but there needs to be more investment in threat intelligence

"Our expertise, as a developer of a DLP solution, extends exactly to this internal threats domain of information security."

-SERGEY OZHEGOV,
CHIEF EXECUTIVE OFFICER,
SEARCH INFORM.

"Mimecast reduces not only the complexity of multiple solution environments, but it also reduces the costs associated with running multiple solutions."

-BRIAN PINNOCK,
REGIONAL MANAGER OF SALES
ENGINEERING, MIMECAST MEA.

"There needs to be more investment in threat intelligence and digital risk management to ensure that they can anticipate cyber-attacks on their customers data, company IP and other critical assets."

-MICHAEL MARRIOTT,
SECURITY RESEARCHER AT
DIGITAL SHADOWS

and digital risk management to ensure that they can anticipate cyber-attacks on their customers data, company IP and other critical assets," said Michael Marriott. "What we have observed is a certain degree of misalignment between investments in tools and technology on one hand, and the requisite human skills on the other. Organizations usually invest more in one over the other, or not enough in either. Enterprises have been spending on security technologies and other infrastructure that either do not work well together, or require a great deal of effort and personnel to follow and address the ensuing multitude of alerts," says Jens Christian HøyMonrad.A single, unified approach will drastically improve the organization's security posture and show companies the true value of all the products they have acquired. "Our advice to CISOs would be to simplify and set their sights on integration across their IT environments. As the number of threats, alerts and security events outnumbers most staff, employed to defend organisations, organisations need to look for solutions which provide not only automation and integration, but also enrich events with tactical, operation and strategic threat intelligence," says Jens Christian HøyMonrad.

The Middle East is alert as compared to other markets regarding shifts in their investment profile in security funding. The best part is that Middle East market doesn't rely much on single vendor cloud based strategies which on the other hand fascinate other markets. "A cloud based strategy is appropriate, but a single vendor cloud approach means that your risk profile rises exponentially.. Mimecast's scalable cloud software-as-a-service model works on a subscription basis when organisations pay per mailbox, rather than outlaying a large portion of funding for costly hardware and software that require regular upgrades," says Brian Pinnock.

THE ROLE OF THE CISO AND CFO

With the threat landscape constantly changing, it is crucial for enterprises to employ structured parameters when planning for organizational security. "It is crucial for CISOs and CFOs to allocate the right resources to protect critical assets. Before setting a security budget, security managers need to assess their current resources and how successful are they with mitigating attacks, and eventually allocate the correct resources to fill in the gaps," said Jens Christian HøyMonrad. Since threat intelligence isn't made equal, it is vital that CISOs and CFOS select intelligence offerings which will aid security operations, ultimately helpingthe businesses in recognizing the risks it is susceptible to.

"A big challenge for business leaders is understanding where they will get the most bang for their buck. Characteristics of a threat intelligence provider should include its coverage, accuracy, timeliness, ease of integration and relevance. Of course, there's plenty organization can do for free. Internal logs and sharing communities can all be useful sources for threat intelligence teams," says Michael Marriott.

FINALLY

The rise of insider threats is definitely becoming an important issue since they arise from unware users whose systems are compromised from top to bottom with malicious insiders who are most likely pocketing a financial gain by selling vital data of the organization, which most likely also includes customer's private data. On the other hand, the External attacker profiles are changing from the outdated hobby hackers to more professional criminal groups, nation states and hacktivists. Enterprises have become extremely alert in the region in order to adapt to this evolving threat landscape and efficiently put their budgeting resources into action to invest in adequate cyber threat intelligence. If organizations fail to meet these criteria, then they can assume an automatic shutdown of their businesses and exit from the competitive market.