Se

WWW.TAHAWULTECH.COM

ADVISOR

BARRACUDA NETWORKS: TOP TIPS FOR SECURING YOUR REMOTE WORKFORCE

INTERVIEW: D-LINK'S HARRISON ALBERT

DDLE EAST

GDPR: TWO YEARS ON

STRENGTH INUNITY

GENETEC'S FIRAS JADALLA ON HOW A UNIFIED APPROACH TO SECURITY DELIVERS UNPARALLELED PROTECTION







Hikvision Temperature Screening Thermal Solutions

SAFER, FASTER, SMARTER





Temperature Screening Thermal Cameras

For more information, please scan the QR-Code to visit our Temperature Screening Thermal Solution page.



CONTENTS

10 Strength in unity

Genetec's Firas Jadalla on how unification enables organisations to become more efficient and resilient

8







PROACTIVE DEFENCE

Fortinet's Derek Manky and FortiGuard Labs' Aamir Lakhani on how to secure a remote workforce

22 GDPR: TWO YEARS ON Industry experts share how the

 Industry experts share how the regulation impacted the digital privacy landscape and how enterprises are coping 28 HIDDEN THREATS What are the risks brough

What are the risks brought by Shadow IT and how can organisations mitigate them?

32 A CISO'S GUIDE TO SURVIVING COVID-19

Top tips on how IT and security leaders can mitigate the cyber risks brought by working remotely



NEXT GENERATION FIREWALL

With all-new Data Security Approach and Contextual Intelligence Engine for security beyond just the perimeter.

FEATURES



GAJSHIELD

GAJSHIELD

G9160m



https://me.dlink.com/



EDITORIAL



Talk to us: E-mail: adelle.geronimo@ cpimediagroup.com

Adelle Geronimo Editor

EVENTS



TIMES ARE A-CHANGING

"It was the best of times, it was the worst of

times...". I'm sure you recognise these lines from one of the greatest novels in history. They are the first lines of Charles Dickens' masterpiece, 'A Tale of Two Cities.' The novel, was set in the time before and during the French Revolution and focused on the magnanimity of those who reached out beyond their own concerns to care and love for others.

While we are not living in a Dickens novel now, in many ways we are living in the best

of times and worst of times.

The coronavirus pandemic has disrupted life as we know it. It has brought significant strains to humanity and the economy.

As we try to navigate the challenges brought by the pandemic, many technology companies offer glimmers of hope as they come together to try to ease the woes brought by the crisis.

Firstly, in connecting people, many technology firms such as Microsoft, Avaya and Zoom have opened their platforms to help people stay connected even while they're practicing social distancing. Secondly, in business, many vendors are helping companies maintain their operations including cybersecurity firms such as SANS Institute are offering free access to security awareness contents; and information security firm Qualys has announced that it will offer its cloud-based remote endpoint protection solution at no charge to its customers for 60 days.

Last, but not least, for public health and safety, tech giants Apple and Google have tied up to develop a contact tracing tool, which utilises Bluetooth technology to help governments and

"MANY TECHNOLOGY Companies Offer glimmers Of hope"

health agencies reduce the spread of the virus, with user privacy and security central to the design. In addition, this month's cover story features Genetec's Firas Jadalla who discussed how the company's Synergis access control

system has been enhanced to deliver insights that can help organisations curb the spread of the virus (see page 10).

On another note, times are a-changing in this editor's life. But one thing's for sure I will be keeping a close a watch on all the exciting innovations that technology and security players will come up with in the coming months and beyond the 'COVID-19 era.'

Stay safe and see you next time!

Published by

CPI MEDIA GROUP

Registered at Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Tel: +971 4 440 9100 Fax: +971 4 447 2409

Printed by Emirates Printing Press LLC, Dubai

> © Copyright 2020 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

FOUNDER, CPI MEDIA GROUP Dominic De Sousa (1959-2015)

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com +971 4 440 9139

ADVERTISING Group Sales Director Kausar Syed kausar.syed@cpimediagroup.com +971 4 440 9130

Business Development Manager Youssef Hariz youssef.hariz@cpimediagroup.com +971 4 440 9111

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com +971 4 440 9128 EDITORIAL Online Editor Adelle Geronimo adelle.geronimo@cpimediagroup.com +971 4 440 9135

> Contributing Editors Daniel Bardsley Mark Forker Giorgia Guantario Sharon Saldanha

DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com +971 4 440 9140

Designer Mhar Delaben marlou.delaben@cpimediagroup.com +971 4 440 9156

PRODUCTION Operations Manager Cherylann D'Abreo cherylann.dabreo@cpimediagroup.com +971 4 440 9107 DIGITAL SERVICES Web Developer Jefferson de Joya Abbas Madh

Photographer Charls Thomas Maksym Poriechkin

webmaster@cpimediagroup.com +971 4 440 9100

SONICWALL TO HELP ACCELERATE MSSPS WITH ENHANCED PROGRAMME

SonicWall has unveiled an

enhanced version of its SecureFirst Managed Security Service Provider (MSSPs) Programme.

The new enhancements are aimed at providing the licensing models, resources and tools needed to help MSSPs profitably scale and accelerate their managed security services business, leveraging SonicWall's awardwinning technology.

Built on the SonicWall SecureFirst Partner Program, the enhanced three-tiered MSSP programme offers benefits such as flexible pricing options, tailored premier technical support access, access to MSSP field sales and technical specialists, increased access to co-marketing funds as well as specialisation training and assessments for sales and technical staff.

"Due to the unprecedented need to quickly and efficiently deploy security to rapidly expanding remote workforces, SonicWall will include its Secure Mobile Access (SMA) solution for MSSPs, allowing managed security service providers to swiftly deploy and scale on-demand security and connectivity at costs based on the number of concurrent users," said Luca Taglioretti, vice president, Global MSSP and Carrier Sales, SonicWall.

Participating MSSPs will continue to be required to meet annual revenue requirements, have a operating NOC or SOC with Help Desk L1/L2 Support capabilities, as well as sales and technical staffing criteria. Authorised MSSPs will need to be established in the SecureFirst programme at the Silver level or above.

UAE LAUNCHES #TOGETHERAGAINSTFRAUD CAMPAIGN AMID COVID-19 PANDEMIC

The UAE Banks Federation (UBF), the Central

Bank of the UAE (CBUAE), Abu Dhabi Police, and Dubai Police have announced the launch of the UAE's first national fraud awareness campaign.

The joint initiative aims to educate and protect consumers from financial cybercrime and fraud, particularly in light of the increased use of digital banking services during the COVID-19 pandemic.

To campaign seeks to encourage UAE residents to remain vigilant while they stay at home. It will be rolled out across social and traditional media channels with the support of the UBF Fraud Prevention Committee and UBF's 53 member banks. Under the theme #TogetherAgainstFraud, content will include educational videos and articles that will raise awareness on how to identify scams and avoid them.

AbdulAziz Al Ghurair, Chairman, UAE Banks Federation, highlighted that the threat financial fraud to society must be addressed, particularly under these challenging circumstances where fraudsters are taking advantage of the fear and ABDULAZIZ AL GHURAIR, UAEBF

uncertainty created by the COVID-19 outbreak.

"With the launch of

this joint campaign we not only aim to equip the public with the knowledge and resources they need to protect themselves from fraud, but also disrupt the criminal networks that are targeting UAE residents. This can only be achieved if we work together, and on behalf of UBF I would like to thank the Central Bank of the UAE, Abu Dhabi Police, Dubai Police and our member banks for their continued support and collaboration. By better preparing banks and customers for the future, we are securing a better future for the entire nation," he said.

The national fraud awareness campaign will run until the end of the year, focusing on different topics every month. These include SIM swap fraud, phishing, vishing, lottery scams, vanishing ink scams, card skimming, email redirection fraud, and data privacy.

QUALYS OFFERS FREE REMOTE ENDPOINT PROTECTION TO SECURE REMOTE WORKERS



Qualys has announced a cloud-based remote

endpoint protection solution at no charge to its customers for 60 days that allows IT and security teams to protect the computers of remote employees.

To enable this free 60-day solution visit, www. qualys.com/remotepatching/. It will initially be available for Qualys customers. Delivery to others will be prioritised based on their signup date. The free Cloud-based Qualys Remote

Protection solution allows security teams to

gain instant and continuous visibility of remote computers, easily see missing patches for critical vulnerabilities and deploy them from the cloud. The patches are delivered securely and directly from vendors' websites and content delivery networks to ensure there is little to no impact on external VPN bandwidth.

If you are a Qualys customer who already has the Qualys Cloud Agent, these systems can be easily enabled to deploy patches via the Qualys Cloud Platform, without the need to touch the client systems. Alternatively, a lightweight Qualys agent is deployed to the remote computers.

Philippe Courtot, chairman and CEO, Qualys, said, "Thanks to our cloud-based implementation, this offer will enable companies to assess in real-time their security and compliance posture and remotely patch employees' devices with the click of a button."

MORO HUB BECOMES DESC-CERTIFIED CSP

Moro Hub, a wholly-owned subsidiary

of DEWA, has announced that it is now a Dubai Electronic Security Center (DESC) certified Cloud Service Provider (CSP) in the UAE.

DESC has developed a CSP Security Standard, which outlines requirements and guidelines for CSPs and those organisations consuming any cloud services. The CSP Security Standard mandates CSPs to comply with international best practices for cloud services. It is based on global information security standards such as ISO/ IEC 27001:2013; ISO/IEC 27002:2013; ISO/ IEC 27017:2015; ISR:2017 v.02 and CSA Cloud Control Matrix 3.0.1.

As part of the extensive DESC certification process, Moro Hub has implemented the Information Security Management System, complying with all international standards for CSPs. These controls were then verified through a comprehensive auditing process by an external certification body appointed by DESC. Ensuring compliance with the CSP Security Standard is a mandatory requirement for CSPs looking to offer cloud services for government and semigovernment entities in Dubai. MOHAMMAD BIN SULAIMAN, MORO HUB



Mohammad Bin Sulaiman, CEO of Moro Hub, said, "The certification demonstrates Moro Hub's commitment to providing secure cloud computing platform and services to our customers. As a DESC certified CSP, our customers know that we have gone through a detailed process to ensure all their cloud service requirements are being met as per superior global standards and best practices. The certification further strengthens Moro Hub's position as customers' preferred partner for their end-to-end cloud service demands."

Moro Hub's cloud operations and data storage infrastructures are fully operational within the UAE. The company's cloud platform is designed to meet the complete privacy and data protection requirements of its customers.

TRA BLOCKS OVER 1000 WEBSITES DUE TO OFFENSIVE CONTENT

The UAE Telecommunications

Regulatory Authority (TRA) has announced that it has blocked up to 1,688 websites in 2019 for using offensive, racist, moral, religious, defamatory and obscene content.

According to a report by state news agency WAM, the TRA also noted that 542 URLs were blocked for obscene content, which accounted for around 32 percent of total sites banned during the year.

Nearly 25.8 percent, or 436, of the websites blocked were used for fraud, in addition to 253 more which tried bypassing web filters. Others were banned for violating intellectual property rights, providing illegal online proxy

18 18 NUMBER OF DAILY COVID-19-RELATED SCAMMING EMAILS SENT TO GMAIL USERS SOURCE: GOOGLE

services and other illegal activities. After discovering a website that provides illegal content, the TRA asks the authorised serviceproviding companies to block the websites and its related pages.

In 2018 TRA banned 2,659 for almost same considerations.

CYBERKNIGHT OFFERS FREE CYBERSECURITY SOLUTIONS AMID COVID-19 PANDEMIC

As a result of the coronavirus pandemic,

organisations around the globe are instituting work/learn from home policies. According to Gartner, "CIOs should prepare IT systems to safely and reliably handle a vast increase in remote workers and digital fulfillment of market demand". Meanwhile, a spike in phishing attacks and ransomware was observed during the outbreak as attackers are using the situation as an opportunity to commit fraud, by impersonating brands to mislead employees and customers. To address regional customer challenges related to budget constraints and making remote working more secure, CyberKnight has launched a special CSR programme which offers a range of cybersecurity solutions at no cost, in collaboration with its vendors. The programme will be available to customers for the duration of the COVID-19 crisis.

Unlimited and free access will be provided for RiskIQ, Flashpoint, Valimail, Immersive Labs, PhishRod and MobileIron.

"Together with our technology partners

VIVEK GUPTA, CYBERKNIGHT

we are coming

together and



finding innovative ways to minimise the impact of cybercrime on the organisations in the region and to limit disruptions to their day-to-day operations. By offering free cybersecurity solutions we aim to help Middle East customers tackle cyberthreats that may be even more prevalent due to remote working during the coronavirus outbreak, while their budgets are being impacted," said Vivek Gupta, Co-Founder and COO, CyberKnight.

PROACTIVE DEFENCE

DEREK MANKY, CHIEF - SECURITY INSIGHTS AND GLOBAL THREAT ALLIANCES, FORTINET **AND AAMIR LAKHANI**, GLOBAL SECURITY STRATEGIST AND LEAD RESEARCHER, FORTIGUARD LABS, DISCUSS HOW ORGANISATIONS CAN PREPARE FOR A SURGE IN ATTACKS TARGETING REMOTE WORKERS.

ver the last weeks, the FortiGuard Labs team has been monitoring a significant spike in coronavirus and COVID-19 related threats. Significant social events are usually a catalyst for new threats to emerge – there are always evil people looking to exploit others during times of crisis – and the current situation is no different.

While this sort of response to the current crisis is not unexpected, what is surprising is the volume of new threats we are seeing in such a short period of time. Trolling the Dark Web looking for new criminal trends, themes, and malware reveals an alarming number of advertisements pitching pandemicrelated scams, such as offers to provide Chloroquine and other medicines and medical devices, all preying on fears Derek Manky, Fortinet

about the current pandemic.

We have also seen an enormous spike in coronavirusrelated scams – money scams, shared riding service scams, money transfer scams, credit card scams, and even scam kits designed for novice cybercriminals known as script kiddies.

Cybercriminals are exploiting the rapid change to our digital world

An unprecedented number of unprotected users and devices are now all online at the same time. In any home, right now, there are likely one or two people connecting remotely to work through the home internet connection. There may also be kids at home engaged in remote learning part of the time and connected to their friends the rest. And the entire family is engaged in multi-player games, talking with their friends in online chat rooms and over social media, as well as streaming music and video. It's a perfect storm of opportunity for cybercriminals.

As a result, the FortiGuard Labs team is seeing an average of about 600 new phishing campaigns per day. Their content is designed to either prey on the fears and concerns of individuals, take advantage of new circumstances, or pretend to provide essential information. These phishing attacks range from scams related to helping individuals deposit their stimulus checks, to providing access to hard to find medical supplies, to providing helpdesk support for new teleworkers.

Aamir Lakhani, FortiGuard Labs

information or even target businesses through their new teleworkers. Which is why the majority of these phishing attacks contain malicious payloads - including ransomware.

viruses, remote access trojans (RATs) designed to provide criminals with remote access to endpoint systems, and even RDP (remote desktop protocol) exploits.

Making matters worse, not every organisation was able to procure enough laptops for every employee who now needs to work remotely. As a result, many teleworkers are using their personal devices to connect into the corporate network. And those devices are not only being use for things like social media, shopping, and streaming entertainment, they are also generally far less protected by desktop security and endpoint protection solutions, which means they are far more vulnerable to the malware being pushed by these phishing attacks. If the device of a remote worker can be compromised. it can become a conduit back into the organisation's core network, enabling the spread of malware to other remote workers.

A sudden spike in viruses

To that point, we have seen a significant rise in viruses, many of which are included in these malicious phishing attachments. During the first quarter of 2020, for example, we have documented a 17 percent increase in viruses for January, a 52 percent increase for February, and an alarming 131 percent increase for March compared to the same months in 2019.

Interestingly, we have also seen a reduction in more traditional attack methods. During the first quarter, for example, we have seen a reduction of botnets per month of -66 percent, -65 percent, and -44 percent compared to the same time period in 2019. Likewise, IPS-based triggers have also dropped by -71 percent in January and -58 percent in March compared to 2019, with a slight uptick in February of 29 percent. This seems to indicate that cybercriminals are adjusting their attack strategies in order to take advantage of the current crisis.

Solutions and countermeasures

It is essential that organisations take measures to protect their remote workers and help them secure their devices and home networks. Consider adopting the same strategy for cyber viruses that we are adopting in the real world. Cyber social distancing is all about recognising risks and keep our distance. Educate your remote workers – and their families

NEW COVID-19-RELATED

PHISHING CAMPAIGNS

ARE BEING FOUND

PER DAY

 about things like phishing and malicious websites and how to stop them. Put security countermeasures in place. Make sure that remote workers have an efficient and effective VPN solution in place. And finally, perform a review of your other security tools. 1

This first tier of threats is designed to take advantage of people

who are either concerned or sitting at home with nothing to do. In addition to online scams targeted at adults, some phishing attacks target kid's computers and gaming systems with offers of online games and free movies, or even access to credit cards to buy online games or shop online stores. Multiple sites are illegally streaming Hollywood movies still in theatres, but also secretly distributing malware to anyone who logs on.

Phishing scams are just the start

While these attacks start with a phishing attack, their end goal is to steal personal

"CYBER SOCIAL DISTANCING IS ALL ABOUT RECOGNISING RISKS AND KEEP OUR DISTANCE."

STATES INSIGHTS ON THE EVOLUTION OF THE PHYSICAL SECURITY

GENETEC REGIONAL DIRECTOR FOR MIDDLE EAST **FIRAS JADALLA** SHARES INSIGHTS ON THE EVOLUTION OF THE PHYSICAL SECURITY SPACE AND HOW UNIFICATION ENABLES ORGANISATIONS TO BECOME MORE EFFICIENT, MAKE BETTER DECISIONS AND STRATEGICALLY RESPOND TO THREATS.

> hen people think of physical security, the picture that often comes

to mind is a heavily guarded building with hundreds of surveillance cameras and doors equipped with access control mechanisms. While this scenario is, in many ways, not far from the truth, the physical security space is evolving rapidly to deliver benefits beyond security.

Driven by the data explosion and increasing digital disruption, physical security tools are now playing key roles in accelerating various business functions from enabling decision-making, improving operational efficiencies to enhancing customer experiences.

This trend has propelled increasing investments in physical security technologies such as IP-based surveillance tools, video management systems and access control solutions. In fact, recent figures released by US-based firm Grand View Research showed that the global physical security market is expected to reach \$171 billion by 2027.

Genetec, a global technology provider of security and public safety solutions, is among the key players that attest to the advantages that these innovations bring beyond generic security. Among the primary solutions that the organisation offers are access control systems.



Today, the solution and the data it generates can play a strategic role in helping organisations to boost not just security but also their productivity, performance and customer satisfaction.

"Access control, which has been in the market for decades, has evolved to become more than just opening and closing doors securely," says Firas Jadalla, regional director – Middle East and Africa, Genetec.

"These tools are now being used to enhance operations management and the data it generates deliver insights that enable organisations to optimise business processes."

An example of an innovative application for access control is in ensuring public health and safety. "Say, if there's a need to evacuate people from a certain facility. Access control systems can be applied to generate reports as to how many individuals there are in certain parts of the establishment and ensure that an effective evacuation measure is carried out," says Jadalla.

According to Jadalla, another vital application of the technology is for accelerating operational efficiencies in manufacturing facilities and airports. "In airports, it can enhance operational management by monitoring the number of people around a certain terminal; it can also record the times logged by each employee during their shifts, which can deliver insights for streamlining various business-critical processes."

In these unprecedented times, while many organisations across the globe are putting significant efforts towards keeping the bad guys away, they are also grappling with a common



and unseen enemy. The coronavirus (COVID-19) pandemic has presented not only a tremendous health crisis but also caused profound social and economic consequences. As a result, many organisations, including those in the technology sector, are devising innovative ways to help contain the spread of the virus. Genetec has recently released a new

PHYSICAL SECURITY

MARKET BY 2027

reporting function for its Security Centre Synergis (Synergis) access control system, which is designed to help organisations find individuals who went through a door that's in close proximity to someone thought to be contagious.

"The feature was developed at the request of McCormick Place in Chicago, North America's largest convention centre," says Jadallah. "The reporting function correlates the physical proximity of an infected individual with other employees PROJECTED VALUE OF GLOBAL and badged visitors based on the use of the access control system." With Synergis, a report



can be quickly generated to correlate access events by time window to identify people who are at increased risk of being in contact with contaminants or contagious individuals.

"Armed with this data, organisations will be able to conduct further investigations as to who are potentially at risk of contracting the virus, notify those individuals and take necessary actions to contain its spread," explains Jadallah.

The feature is being offered by Genetec to its access control customers at no extra costs. As for its regional applications, Jadalla believes that there is a strong demand for this kind of solution.

"The Synergis proximity report feature will definitely be instrumental in helping regional firms curb the spread of COVID-19 or any kind of contagion," says Jadalla. "We can customise the solution depending on the needs of the end-user but, ultimately, these reports can help them proactively take the necessary precautions."

A unified approach

The evolution of the physical security space has paved the way for increased integration between multiple security components such as video surveillance, access control, intrusion detection and analytics to deliver a holistic security infrastructure to organisations. However, the result often remains a set of disparate systems that lack interoperability.

"Having a unified system helps enterprises to maximise the usage of their security infrastructure, make seamless upgrades and enable unified "HAVING A UNIFIED SYSTEM HELPS ENTERPRISES TO MAXIMISE THE USAGE OF THEIR SECURITY INFRASTRUCTURE, MAKE SEAMLESS UPGRADES AND ENABLE UNIFIED THREAT LEVEL MANAGEMENT."

threat level management," says Jadalla.

He adds, "What this means is organisations will be able to vastly improve their physical security management using one platform, with a single interface. With unification, these systems can communicate with one another and generate actionable insights that can be leveraged and combined with operational data to help improve efficiency."

With unification, organisations no longer need to worry about upgrades. "Normally if you integrate different systems, once you upgrade you break the link," explains Jadalla.

Security tools too are vulnerable to cyber-attacks since organisations with multiple integrated systems often utilise tools from various vendors and platforms. However, with a unified solution like Genetec's Security Centre, cybersecurity is applied – and updated – across all physical security components. The solution is a unified security platform that blends IP security systems within a single intuitive interface to simplify operations.

"A unified system is easy to manage and more cost-effective to deploy," says Jadalla. "We believe that unification is going to be the future for security."

3 FACTORS TO CONSIDER IN SECURING YOUR REMOTE WORKFORCE

TONI EL INATI, RVP SALES, META & CEE, BARRACUDA NETWORKS, SHARES INSIGHTS INTO HOW ORGANISATIONS CAN ENSURE THE SECURITY OF THEIR REMOTE WORKFORCE AMID THE CORONAVIRUS PANDEMIC.

he coronavirus (COVID-19) pandemic has turned social and business interactions across the world upside down.

Increasing concerns over the implications of the crisis have led organisations to rethink their strategies and take unprecedented actions to ensure business continuity. As a result, many companies have opted to close their physical operations and implement remote working models. This massive surge in telework has placed tremendous stress on corporate IT infrastructures.

As companies juggle a range of new priorities, from ensuring employees' health and safety, maintaining sudden changes in IT systems to ensuring business continuity, cybercriminals are positioning themselves to take advantage of the uncertainties brought by COVID-19.

When your entire workforce is working remotely, any thoughtless action could bring disruptions across the organisation as security becomes volatile. Organisations then need to put significant focus on the cybersecurity of their remote teams, to ensure not only the protection of corporate data but also the survival of the business.

Here are the top three factors organisations need to consider to ensure

the security and productivity of their remote workforce:

Email security

Since the outbreak began, we have witnessed a significant spike in COVID-19related phishing scams. Barracuda has further observed a recent spike in this type of attack, which rose to 667 percent since the end of February.

One of the most common types of these attacks is an email impersonation attack. In this attack, cybercriminals impersonate organisations such as the World Health Organisation (WHO) or even charitable institutions to trick users into opening a malicious email. Multiple government firms have issued warnings against these attacks. Unfortunately, people today are desperate to find out more about the crisis and are letting their guards down, clicking on just about anything sent to them.

In order for organisations to ensure that their workforce is secured against such attacks, it is imperative that they implement the best email security posture by having a multi-layered defence approach.

Enterprises can leverage solutions such as Barracuda Essentials, which delivers advanced Office 365 security features including email scanning, archiving, backup and recovery.

Employees are the first line of defence for any organisation, hence, it is vital that they are equipped with the tools and knowledge against threat actors. Barracuda also offers Barracuda PhishLine which enables companies to develop security awareness programmes in order to guard against a range of threats with patented, highly-variable attack simulations.

Cloud-to-cloud backup

Millions of employees have moved from corporate workspaces to home offices, which has created a handful of challenges that can have a negative impact on data protection.

Working from home, employees are inevitably going to be focusing on other things – their children, pets, health concerns, finances, etc. – which may disrupt their normal pattern of accessing and saving files. Moreover, employees accessing and saving data from a variety of endpoints and applications increase the risk of accidental deletion and falling victim to cyber-attacks. With strict regulations set in place for the storage, management and use of data, organisations cannot afford to be lax on their data protection and backup strategies.

Barracuda's Cloud-to-Cloud Backup allows corporate data to be accessible, searchable, and recoverable from anywhere with an internet connection. By leveraging this solution organisations will be able to protect their collaborative workspaces as well as optimise data security and backup.

Web Application Firewall

As more and more customers rely on online stores and services, it is imperative for businesses to ensure that their applications can scale rapidly to meet the sudden influx of demands. However, for many companies, the move to remote working came too rapidly, which left them with little time to prepare for the cybersecurity challenges.

Applications remain one of the most commonly exploited threat vectors, especially as organisations bolster their online presences. Deploying a Web Application Firewall helps protect applications, APIs, and mobile app backends against a variety of attacks. Unfortunately, oftentimes configuring traditional WAF can take days of effort. Moreover, businesses tend to struggle with web application security due the complexities of managing WAF and the resources required to do so.

To address this challenge, especially during this trying time, companies can leverage Barracuda WAF-as-a-Service, which makes it easy and cost effective for customers to stay protected against advanced layer 7 attacks such as DDoS, bots, zero-day threats, OWASP Top Ten, and more. Barracuda WAFaaS also provides IT

> To find out more about how Barracuda Networks can help protect your remote workforce, visit: https://www.barracuda. com/covid-19-security

"ORGANISATIONS THEN NEED TO PUT SIGNIFICANT FOCUS ON THE CYBERSECURITY OF THEIR REMOTE TEAMS, TO ENSURE NOT ONLY THE PROTECTION OF CORPORATE DATA BUT ALSO THE SURVIVAL OF THE BUSINESS."

leaders with complete control and gives them granular visibility into application traffic, which allows them to gain valuable insights that not only to ensure total application security but also enable strategic planning.

Conclusion

With the coronavirus not showing any signs of slowing down anytime soon, organisations need to take the necessary steps to protect two of their key assets – their data and employees. But ultimately, as companies adapt to this new style of working, it is imperative that they deploy tools that do not only bolster security postures but also enhance operational efficiency and accelerate business performance. **1**

Toni El Inati, Barracuda Networks

SECURING THE NETWORK

D-LINK MIDDLE EAST AND AFRICA REGIONAL DIRECTOR **HARRISON ALBERT** DISCUSSES THE COMPANY'S STRATEGIC PARTNERSHIP WITH NETWORK SECURITY FIRM GAJSHIELD, AND HOW THEIR COLLABORATION CAN HELP ENTERPRISES PROTECT NETWORKS AND PREVENT DATA LEAKS.

an you please elaborate on D-Link's partnership with GajShield?

D-Link's strategic partnership with GajShield open the doors to partners in the Middle East and African market to reach the SMB and enterprise segment by empowering them with the bestof-breed solutions for network and data security. D-Link's vast market intelligence enables Gajshield to evaluate their products against the market's needs, allowing them to deliver the latest technological trends and develop future-ready products.

Harrison Albert, D-Link MEA

What differentiates GajShield's solutions from its competitors in the market?

Data today is a very important aspect of any organisation's security measure and data leak prevention is a top priority for CISOs. GajShield Firewalls have an integrated Context-Based Network Data Leak Prevention that helps organisations secure data and prevent both intentional and unintentional data leak across various web, cloud and Software-as-a-Service (SaaS) applications. This solution combined with Gajshield's remote working solution Enterprise Cloud, allows organisations to ensure data security even with the remote and roaming users.

What are the key elements driving the demand for more sophisticated network security solutions? How are D-Link and GajShield addressing these demands?

Organisations today have moved beyond just the network and use of multiple cloud/web application for data sharing and storage for enhancing business operations. The recent adoption of remote working has brought out the fact that the network boundary is vanishing and defending it demands a more sophisticated security solution that does not only protect the network but also guard corporate data.

GajShield addresses this demand by taking an all-new Data Security Approach. This approach keeps data at the core of all its security measures and at the centre of security policies.

Unlike traditional security methods, Gajshield's Data Security Approach uses Contextual Intelligence Engine that leverages the Layer 7 application visibility, which delivers deeper intelligence to prevent data exploitation.

According to IDC, there will be 41.6 billion IoT devices in the field by 2025. How important are next-gen firewalls in securing the connected era?

Internet of Things (IoT) technologies will be a crucial part of our future daily lives. They will also be the most targeted devices by cybercriminals if left unsecured, these devices will be used as a gateway to enter one's network and take control of their whole ecosystem. We have seen such attacks in the past and it will only grow in the future. Cybercriminals will use these hacked systems to perform DDOS attacks on various organisations. Additionally, these devices can also be leveraged to mask various other attacks. Hence, using a firewall will be vital in preventing cyber-attacks that could have real-life harmful implications to people utilising IoT devices.

The current COVID-19 pandemic has pushed organisations to implement work-from-home strategies, which puts significant security strains to corporate networks. How can GajShield's solutions strengthen organisations' network security and help stem data leaks?

COVID-19 has changed the way we work. With the adoption of work from home models, enterprises are facing challenges with not only securing the remote users but also preventing "THE RECENT ADOPTION OF REMOTE WORKING HAS BROUGHT OUT THE FACT THAT THE FACT THAT THE NETWORK BOUNDARY IS VANISHING AND DEFENDING IT DEMANDS A MORE SOPHISTICATED SECURITY SOLUTION."

data loss, whether it's by accidental or intentional data leaks. GajShield Enterprise Cloud Solution enforces the traffic of these remote users through the Head Office's Firewall (public or Private) and applies data and network security policies on these users. This helps in monitoring and controlling of data transactions across Web. SaaS and Cloud applications like Gmail, Yahoo, Rediff Mail, Google Drive, OneDrive, File Transfer applications like We Transfer and various Social Media Platforms. This also prevents Shadow IT and gives organisations the ability to control access to various application and restrict them for business use only. Enterprise Cloud also allows the organisation's Cybersecurity team to enforce security policies to restrict access to malicious applications and URLs that poses as a threat to the organisation. 1

PRIME TARGETS

WHALE PHISHING OR CEO FRAUD CAN AFFECT ANY TYPE OF COMPANY, FROM SMALL FAMILY BUSINESSES TO LARGE MULTINATIONALS. INDUSTRY EXPERTS SHARE INSIGHTS INTO HOW THIS CYBER-ATTACK WORKS AND HOW TO PREVENT IT. here are few things better designed to make an employee panic and than an email from the boss marked "urgent". With adrenaline levels high, a staff member can easily act rashly by doing as the



John Shier, Sophos

"UNFORTUNATELY THERE DOESN'T SEEM TO BE ANY MEANINGFUL REDUCTION IN THE ← AMOUNT OF BEC, SINCE IT REPRESENTS A RELATIVELY EASY AND EFFICIENT WAY FOR CRIMINALS TO MAKE MONEY."

This was an attempt at CEO fraud, and such emails are often successful because they deliberately push a series of buttons.

Firstly, these tend to be aimed at the finance department of companies, where there may be less awareness of the risk of cyber fraud than there is in the security or IT department.

The fraudsters will ask the customer to make payment for an invoice into their own bank account, not the account of a genuine supplier to the company.

As indicated by the example Trost encountered, there is often a sense of urgency about these requests, says John Shier, a senior security advisor at Sophos, which offers AI-driven and cloud-native security solutions.

The wider field of Business Email Compromise (BEC), of which CEO fraud is one type, is often characterised by a refusal to communicate by telephone, with fraudsters instead insisting on email instead.

The scale of the fraud can be eye watering, with single cases of money being transferred into the wrong account sometimes reaching hundreds of thousands of dollars or more.

Indeed, BEC and email account compromise (EAC) was, according to the United States' Federal Bureau of Investigation, responsible for \$26 billion of losses between July 2016 and July 2019.

"Unfortunately there doesn't seem to be any meaningful reduction in the amount of BEC, since it represents a relatively easy and efficient way for criminals to make money," says Shier. "As companies increasingly adopt cloudbased email services, this arguably makes it even easier for criminals."

In the past, says Shier, criminals had to carefully craft their campaigns by forging email addresses and domain names, or even gaining access to internal resources.

"Now, they simply need to phish their target for email account credentials and carry out their crime entirely inside the inbox," he says.

Criminals are using the coronavirus outbreak to find new ways to attack companies. Morey Haber, chief technology officer and chief information security officer at BeyondTrust, the privileged access management cybersecurity company, says that an email might, for example, say that a company's Singapore office has been asked to close because of the pandemic. It then requests the user logs into a government portal.

"You click on the link – it's malicious," says Haber.

The starting point for many attacks targeting employees is social media research by the fraudsters.

LinkedIn, Facebook and the like offer details about individuals in a company, including job titles, families and interests.

Kamel Heus, regional director for Northern and Southern Europe, the

message asks and paying an invoice.

However, sometimes such emails are from criminals attempting to steal money and are not, as they initially appear to be, from a top company executive.

Ryan Trost, co-founder and chief technology officer of the threat intelligence platform ThreatQuotient, encountered these scenarios earlier in his career when he managed a large security operations centre.

"An adversary was masquerading as a senior vice president and sent an email to several employees in our accounts payable department," explains Trost.

"Although the fictitious email address was a Gmail account, the adversary was able to manipulate the email envelope field and include the VP's real email address to better camouflage the attack."

The email included a fake invoice and asked for a wire transfer to be expedited to avoid a steep late fee.

The spearfish was well crafted, being direct and authoritative with proper grammar, and the vice-president's legitimate email signature. It went to all employees necessary to approve a wire transfer.

What gave the game away was that, at the bottom of the email, the vicepresident's nickname was not included as it should have been. As Trost puts it, "a minor but obvious nuance."

"This personal level of detail is usually hard for adversaries to mimic and is commonly overlooked," he adds. Middle East and Africa at Centrify, says fraudsters use this information to establish trust.

As well as requesting employees to click a link or send money to a bank account, fraudsters might ask for gift cards to be purchased or a (malware) attachment to be opened.

"Some sophisticated hackers may buy lists of user credentials from the dark



Kamel Heus, Centrify

"DON'T JUST CLICK ON SOMETHING BECAUSE YOUR CEO HAS ASKED YOU."

web and identify targets who are most likely to have privileged access to some or all of the organisation's sensitive infrastructure or data that could be exploited," says Heus.

Fraudsters even hack social media accounts of friends of their target person, says Israel Barak, chief information security officer at the Boston-based cybersecurity company Cybereason.

"That gives you a perspective of how targeted these attacks are, when they've done their research on social networks and made the effort of compromising a password of one of these first-degree contacts and act as if they are that person," says Barak.

Trost once encountered an attack when fraudsters, after researching the company CEO online, pretended to be his daughter asking him to proofread a college paper. By planting malware in the paper, the fraudsters hoped to gain access to the executive's laptop.

"Luckily our malware sandbox flagged the email as suspicious and we were able to open an investigation," says Trost.

Such attacks aimed at the CEO or other

top executives (rather than pretending to come from him or her) are known as whaling. Busy and privy to sensitive information, C-suite executives are seen as prime targets.

So ,what can be done about CEO fraud and whaling? While police forces in the UAE have capabilities focused on combating cyber fraud, getting money back that has been paid out to fraudsters is extremely difficult.

Therefore, prevention is vital, and multiple measures can be taken. A key one is to have a questioning mindset.

"Don't just click on something because your CEO has asked you. Make sure the sender's email is legitimate and check the links to confirm that they are genuine and recognised links," says Heus.

"Even if the email has a personal touch to it, does it come with an abnormal request? Would your CEO really ask for your password. Pick up the phone and verify the request."

Particular awareness is needed in the current climate, says BeyondTrust's Haber.

"Training for phishing in general and whaling has been pretty good. The twist has been because of Covid-19, people are hungry for information. They're more gullible for a social engineering attack based on the crisis. That's pushing the training aside," he says.

"We have to say, 'Your training about phishing and whaling and spear phishing, that doesn't go away.""

Barak at Cybereason notes that multifactor authentication should be used to ensure email addresses are well protected.

He also says a "post-breach" mindset is important, as some attacks will succeed. This means having visibility as to what is happening on executives' machines to identify abnormalities.

Security operations teams should be "abundantly cautious" when defending against spearphish attacks, says ThreatQuotient's Trost. As well as training, measures include inbound non-corporate keyword notifications for emails and malware analysis sandboxing.

"There are no silver bullet defences to block all spearphishing attacks, but security operations teams can implement several layered defences to help detect and block spearphish attacks," he says.

CUFY SECURITY

eufyCam 2 1080p Wireless Security Camera

Protects You, Your Family and Your Privacy



Night Vision

Weatherproof IP67-Rated

48HRs **Backup Battery for** HomeBase



Live Streaming

100dB Siren Anti-Theft Protection

1080_P

Full HD

Amazon Alexa

AES 256

CUFY

FREE

ENCRYPTED LOCAL STORAGE

SECURITY



1 Charge =

Davs



Goog<mark>l</mark>e Assistant



Apple

Home Kit

eufy Security Range of Products



eufyCam 2 2+1 kit T8841



eufycam 2C 2+1 kit T8831



eufy Floodlight Cam T8420



eufy Doorbell 2K with Homebase E8210



Available at









FEATURE

GDPR: **Second Second Se**

THE ENACTMENT OF THE GENERAL DATA PROTECTION REGULATION (GDPR) IN MAY 2018 HAS PUSHED MANY ORGANISATIONS TO RE-THINK THE WAY THEY MANAGE, UTILISE AND PROTECT DATA. WITH ITS SECOND ANNIVERSARY FAST APPROACHING, HOW HAS THE REGULATION IMPACTED THE DIGITAL PRIVACY LANDSCAPE AND HOW ARE ENTERPRISES COPING? DANIEL BARDSLEY INVESTIGATES.





wo years ago this month, Security Advisor Middle East posed a stark question on its front cover, asking, "GDPR: Are you ready?" It was on May 25, 2018 that the General Data Protection

Regulation took effect, so the hope is that organisations have by now come to terms with the brave new world heralded by the far-reaching rules.

The European Union, which is behind the regulations, has clearly been taking them seriously, because multiple heavy fines have been levied for breaches.

The legislation states that organisations can be fined up to EUR 20 million (AED 79.9 million) or four percent of their annual turnover, whichever is greater, for transgressions.

As of late April this year, well over 250 fines had been levied – excluding any that may not have emerged publicly – and while many have been for just a few thousand euros or less, others have involved eye-watering sums.

In the most serious cases so far, British Airways had its wallet lightened to the tune of more than EUR 200 million, Marriott International Hotels by slightly above EUR 110 million and Google by EUR 50 million.

GDPR was introduced in the wake of multiple cases where the data of consumers had been leaked.



Brian Chappell, BeyondTrust

"IT'S BEEN A ROUGH ROAD AND MANY COMPANIES ARE STILL NOT THERE WITH THEIR COMPLIANCE, BUT THOSE THAT HAVE TAKEN THE JOURNEY ARE LIKELY TO BE STRONGER AS A RESULT." Aside from the headline-grabbing fines, and the many other smaller penalties, what has the implementation of GDPR meant for companies? An interesting analysis of this came from a paper published earlier this year by Digital Europe.

Entitled Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework, the report notes that the legislation has sparked widespread investment in data compliance across industry.

As well as aiming to cut the risk of data breaches, the legislation strengthens the hand of individuals when it comes to determining how their data is stored and used.

As a result, organisations have had to look at how they collect, store and retain data to ensure that they do this only where necessary, and have been forced to assess the relevance and need for the data that they control.

Brian Chappell, director – project management at BeyondTrust, the privileged access management cybersecurity specialist, says that many companies collected data without a clear idea of how it would be used. While they may have thought that it might prove useful down the line, such "hoarding" conflicts with GDPR and other recent data protection legislation.

"Companies have had to review their need for data and ensure that, where it's collected, they have clear permission for the uses the data was intended for as well as controls to delete the data once its processing was complete," says Chappell.

While this might be seen as an additional administrative burden, Chappell says that complying with the legislation offers spin-off benefits.

"The need for audit trails around who has access to data and who has accessed data leads to overall better security practices. It's been a rough road and many companies are still not there with their compliance, but those that have taken the journey are likely to be stronger as a result," he says.

Indeed, in some companies, GDPR has resulted in the wholesale updating of IT systems after executives realised the importance of compliance.

A multi-stakeholder group that reported to the EU as part of a "stocktaking" exercise in June last year said in a report that, in this way, "GDPR was often seen as effecting positive change".

"Many organisations welcomed the spur of GDPR in obtaining funding and management buy-in for finally updating IT systems that have for some time needed to be upgraded," the report said.

Despite such positive outcomes, many companies have not completed the necessary work to manage their data appropriately two years on from the legislation's debut, according to Chappell. Some, he says, have not even started, labouring under the misapprehension that GDPR does not apply to them.

A key point is that organisations in the Middle East are not immune to the rules or the risk of fines just because GDPR is EU legislation. The reach of the regulations extends far beyond the EU because any organisation, regardless of where it is based, comes under GDPR's remit if it offers goods or services to individuals within the EU.

While GDPR has sometimes sharpened up company procedures when it comes to customer data, concerns have been raised over its implementation.

In particular, the Digital Europe report indicates that the rules may have in some instances been interpreted more strictly than was intended.

The report says that there is "a clear tendency" from data protection authorities and the European Data

Protection Board "to put forward an overly restrictive interpretation of the legal framework". In some instances, the report states, this has gone "against the letter and spirit of the GDPR text or relevant case law". Innovation and investment could be harmed as a result.

Other concerns centre on companies producing long and complex data protection declarations, which is at odds with the legislation's aim of improving transparency.

Digital Europe says that there have also been worries about unnecessary data requests, such as from former

"AS OTHER DATA PROTECTION REGULATIONS COME INTO EFFECT, THE EFFORT IN COMPLYING IS LIKELY TO BE INCREMENTAL AND PROBABLY MINIMAL IF YOU ARE ALREADY GDPR-COMPLIANT."

employees of organisations, and that organisations have been informing data protection authorities too often about minor data breaches.

Another challenge that companies grappling with GDPR may face is, says Chappell, its openness, as it does not prescribe exactly what must be done to protect data.

This is particularly difficult for companies with limited data management functions and it is where outside assistance may be useful.

"Engage with GDPR specialists who can help guide the organisation towards compliance," he suggests.

When the use case for collecting or processing data is unclear, Chappell says

companies should ask themselves "hard questions" about whether that use case is essential for their business.

Although GDPR already applies to the actions of many companies in the UAE and the rest of the GCC, legislative changes will redouble the importance to them of good data practice.

In 2018, Abu Dhabi Global Market (ADGM) brought in new data protection rules, while in August last year, Bahrain introduced its data protection law. Also in 2019, Dubai International Financial Centre launched a consultation about plans to amend its own data protection law, changes that are due to be introduced this summer. There are also proposals for a UAE-wide data protection law.

Many new data protection rules being introduced around the world have used GDPR as their foundation, so the long reach of GDPR is set to extend further, albeit indirectly. Companies that are already up to speed with GDPR may welcome the fact that other jurisdictions are using the EU legislation as a blueprint.

"As other data protection regulations come into effect, the effort in complying is likely to be incremental and probably minimal if you are already GDPRcompliant," says Chappell.

In today's global market, Chappell says that companies that think of themselves as regional are more likely to find themselves with customers from many disparate countries.

"The question then becomes whether you want to be the company that is rushing to comply with the data protection regulations of a new customer's country, or do you want to be the company that takes data protection seriously and has already adopted GDPR practices and is ready to deliver?" he says.

So, two years on, GDPR is still raising questions for companies in the Middle East.

Barracuda Cloud Security Guardian

Build fast. Stay secure.

Remove security as a burden in the cloud.

Developers like the speed and flexibility of the cloud—but many fail due to cloud security challenges. Cloud Security Guardian manages security for them, automatically.

Leverage industry best practices for security compliance.

Cloud Security Guardian is fully CIS Benchmarks-certified – their benchmarks are incorporated as pre-loaded policies in Cloud Security Guardian. Policies for PCI DSS and HIPAA are also included.

Full-stack cloud security.

Only Barracuda Networks integrates cloud security management with perimeter and network security solutions – i.e., control, data, and management plane security together in a single solution.

For more information visit: barracuda.com/products/cloudsecurityguardian or contact: MET_sales@barracuda.com

80 percent of cloud breaches are self-inflicted.

"Through 2020, 80 percent of cloud breaches will be due to customer misconfiguration, mismanaged credential, or insider theft."

Gartner Research



THE REAL COST OF FIGHTING INSIDER THREATS

AS THE DEFENCE AGAINST INSIDER THREATS IS BROAD, LAYERED AND VARIED, SO TOO ARE THE COSTS INVOLVED, SAYS **EMILE ABOU SALEH**, REGIONAL DIRECTOR, MIDDLE EAST AND AFRICA, PROOFPOINT.

nsider threats are on the rise: up 47 percent year-on-year and organisations are paying a heavy price. According to the latest Cost of Insider Threats 2020 Global Report, impacted organisations in the Middle East spent on average \$11.65 million annually on overall insider threat. Moreover, regional enterprises have experienced the highest number of insider-related incidents over the past 12 months, and are likely to experience credential theft.

Figures of this magnitude can be difficult to relate to. But for the organisations behind them, the impact of an insider threat is incredibly real. Costs quickly arise from additional labour and investment in technology, through to business disruption and revenue loss. As with external threats, attackers' tactics and motives differ. Unlike outsidein attacks, attackers do not need to breach defences, and many are unaware they're a threat at all – making them hard to profile, harder to detect and extremely difficult to defend against.

Insider threats – be they intentional or not – cannot be entirely avoided. That's not to say that businesses must accept these costs, however. By taking a proactive approach, through costeffective tools and training, incidents can be minimised, and costs controlled.

The financial reality of insider threats

As the defence against insider threats is broad, layered and varied, so too are the costs involved. From the proactive, monitoring and surveillance, to the reactive, post-analysis and remediation, an insider threat impacts numerous activity centres across an organisation.

Threats must be thoroughly investigated to determine the source and scope, escalation and planning meetings are required to inform all necessary stakeholders, and a response strategy must be put into action. All of which carries a substantial cost. As a result of a single insider threat, organisations spend around \$22,000 on monitoring and surveillance and \$125,000 on investigation and escalation.

All this before accounting for the costliest part of the operation: containment. Containing an insider incident accounts for one-third of Emile Abou Saleh, Proofpoint

PR disaster and damage to reputation and stakes are seldom higher. The most effective way to avoid such substantial financial consequences is to minimise the risk of an insider threat occurring in the first place. While proactive measures also carry a cost, it is always better to spend a penny on prevention than a pound on cure.

Unfortunately, many organisations are lacking in this area. Training, while prevalent, is often inadequate and the methods used are rarely the most cost-effective.

The current battleground

The recent State of the Phish report found that 95 percent of organisations around the world undertake some form of cybersecurity training with employees. Unfortunately, under further examination, the content, frequency and methods used are found wanting.

For most employees, security training totals just three hours over the course of a year. Many organisations only train a portion of their users and do not carry out in-person sessions or simulated attacks.

As a result, much of the workforce is uneducated about common cyber threats. Just 61 percent could correctly define phishing, with only 31 percent recognising ransomware and 66 percent familiar with malware. Against this backdrop, the rise in negligent insiders makes perfect sense. When it comes to preventing insider threats, most organisations opt for a combination of user training awareness, data loss prevention, and user behaviour analytics to educate and equip staff.

By far, the most cost-effective method of minimising and managing insider threats is a combination of awareness training, user behaviour analytics, and privileged access management (PAM) – the latter reducing average costs by \$3.1m. Despite this, PAM is only deployed by 39 percent of organisations.

Don't be left counting the cost

All organisations must implement a comprehensive and effective insider threat management program, to deter, detect and defend against rising numbers of incidents.

The most effective way to avoid the damage caused by insider threats is to prevent them where possible. Use the tools available to flag suspicious activity, block unusual access requests and ringfence sensitive information and privileged credentials.

Training and education are just as important. Ensure that your users are aware of common threats, that they understand how their behaviour can increase the likelihood and success of attacks, and that they understand their role in defending against these threats.

If an attack is successful, containment is key. The faster an incident is contained, the lower the cost. Ensure protocols and protections are in place to identify and rectify any incident as soon as possible.

Before, during and after an insider threat, vigilance and responsiveness are vital. The better you know your people, your environment and your systems, the better you can protect them from threats – whether they're knocking at the door, or already inside.

the total costs involved, at approximately \$211,000. Closely followed by remediation at \$147,000 and incident response at \$118,000.

Unsurprisingly, technology and labour are the two largest cost categories, accounting for almost half of the total outlay between them. This covers overtime, additional personnel, contractors and any software and hardware needed to remedy the situation.

With the scope of a single incident laid bare, it's easy to see why insider threats can be so destructive. Add a potential

"THE MOST EFFECTIVE WAY TO AVOID THE DAMAGE CAUSED BY INSIDER THREATS IS TO PREVENT THEM WHERE POSSIBLE."

HIDDEN THREATS

WITH THE INCREASING NUMBER OF EMPLOYEES BRINGING THEIR DEVICES TO WORK AND UTILISING NEW SOFTWARE SOLUTIONS AND CLOUD SERVICES TO BOOST PRODUCTIVITY, SHADOW IT IS BECOMING ONE OF THE MOST COMMON PROBLEMS COMPANIES FACE TODAY. SECURITY CORRESPONDENT DANIEL BARDSLEY SPEAKS TO INDUSTRY EXPERTS ON THE RISKS OF SHADOW IT AND HOW ORGANISATIONS CAN MITIGATE THEM.

5

6

att Walmsley remembers well a meeting he was once in with the chief information security officer of a major company with

thousands of employees.

The CISO, says Walmsley, who is head of EMEA marketing for the cybersecurity company Vectra, thought that there were seven to 10 logins for Office 365 in the company. In fact, there were 78.

"He was completely blindsided," says Walmsley, adding that such lack of awareness of the IT assets in a company is "not unusual".

This is the world of shadow IT, of applications and networks built up alongside the official assets of a company that are overseen by the main IT department and cybersecurity staff.

Departments sometimes want to buy their own IT assets or services in order to cut through bureaucracy and save time. But shortcuts may bring risks.

As Marco Rottigni, chief technical

security officer EMEA at Qualys puts it, shadow IT can be "unknown, unmanaged, unprotected and potentially risky".

"The teams that do the administration don't have the skills, competence and knowledge to provide the security to mitigate these risks," he says.

"This is why the security department exists, the compliance department exists."

So, what are the security risks linked to shadow IT? Adam Palmer, the chief cybersecurity strategist at the cybersecurity company Tenable, says that lack of visibility is a key issue.

"Security teams often struggle to identify all assets connected to the corporate network. You can't protect new devices if no one knows they are on the network. These assets may be insecure or obsolete," he says.

The IT department's various firewalls and other security devices may not be protecting shadow IT assets, and there is no guarantee that software updates and the like are regularly being installed.

Other concerns centre on data, with cloud storage being especially vulnerable to attacks and breaches.

An interesting historical perspective



Adam Palmer, Tenable

"YOU CAN'T PROTECT NEW DEVICES IF NO ONE KNOWS THEY ARE ON THE NETWORK."

on the issue of shadow IT (or stealth IT and rogue IT, to use other popular terms) is offered by Dr Mike Lloyd, chief technology officer at the cyber risk modelling company RedSeal.

"We've seen the pendulum swing between centralisation and decentralisation for decades," he says.

Early on, when mainframe computers held sway, things were easy to control, but that changed with the PC revolution, which allowed departments to take care of their own IT needs. When floppy disks became agents for the spread of viruses, central control was reasserted.

"The reason the pendulum keeps swinging is we need to find this Goldilocks balance between freedom and flexibility," says Lloyd.

Now, in the era of the cloud, the pendulum has decisively swung back in favour of shadow IT, with a simple credit card now enough to purchase and to start using services.

As Vectra's Walmsley puts it, "the technical and time barriers" to setting up shadow IT "have been dramatically removed".

There is also the phenomenon of "Bring Your Own Device", in which employees use their own mobiles and other hardware.

Shadow usage of the cloud is "a massive issue", according to Ted Demopoulos, a principal instructor at the cybersecurity training organisation the SANS Institute, especially as many cloud providers offer free basic-level application functionality and storage.

"The temptation for users to take

advantage of this free functionality is very high, and many do not even know they should not be using it," he says.

Concerns about cloud-based shadow IT assets are also raised by Mouli Srinivasan, product consultant at ManageEngine. If shadow IT is not monitored effectively, he says there is a "frighteningly high" probability of data leaks and data loss.

He offers a real-world example to illustrate the point. A finance director might share a root-level folder (a folder with privileged access) with an employee through a third-party cloud file storage application.

If this app has permission to look through all of the related files and folders

regulatory law, protected appropriately. However, unknown to everyone, there was another copy of this data in a test bed which was not protected appropriately," he says.

Such issues are a particular concern in today's environment, in which the likes of the EU's General Data Protection Regulation (GDPR) can result in significant fines for companies that fail to keep a proper control on data.

Highlighting a different potential data-related risk, the network monitoring company Paessler notes in a briefing document that there may be no back up to shadow IT storage, raising the risk that crucial data could be lost.



Ted Demopolous, SANS Institute

"THE TEMPTATION FOR USERS TO TAKE ADVANTAGE OF THIS FREE FUNCTIONALITY IS VERY HIGH, AND MANY DO NOT EVEN KNOW THEY SHOULD NOT BE USING IT."

being shared, this might inadvertently provide access to detailed financial statements under the root folder.

"Thus, the finance team's files, folders and discussions might end up being controlled by a third party," says Srinivasan.

"Worse, if leaked to the public, that information could be indexed by search engines, making your internal files, like salaries and profit-and-loss statements, public."

Demopoulos at the SANS Institute says that there are also risks linked to "shadow copies" of data, even if does not come under the definition of shadow IT applications and infrastructure.

"For example, one client had sensitive data, which was also governed by

Given the risks associated with shadow IT, what should companies do to keep control of it? Demopoulos highlights the importance of training so that employees understand what they may and may not do.

"The biggest control here is simply setting a security policy and making sure people know about the policy," he says.

"So many users of shadow IT claim, rightfully or not, that they did not know that what they were doing was not allowed."

Specialists say, however, that efforts to keep control of shadow IT should, as far as possible, not be at the expense of business flexibility.

"What can you do to minimise the risk of Shadow IT without disturbing

the purpose for which Shadow IT is adopted?" says Rottigni at Qualys.

"As a security practitioner, I'm not against Shadow IT adoption. Maybe they will have a better idea for executing a task. Maybe the personal initiative brings innovation."

The question becomes, says Rottigni, how to ensure that assets are visible without disturbing the adoption of valuable shadow IT.

It is a view echoed by Tenable's Palmer, who says that "functionality must always been considered" when implementing measures such as network segmentation, which might be used to restrict access to key systems only to known secure devices.

"One of the biggest reasons people turn to Dropbox for file sharing, Gmail for email, or AWS for infrastructure is because these services enable them to do their jobs more efficiently and effectively," he says.

"Blocking certain cloud applications or shadow assets may help eliminate the technology problem, but it won't solve the business problem."

In this context, Palmer advises security departments to recognise that employees will use these types of popular services and "implement a security programme that eliminates security blind spots".

"Security requires a deep, real-time view into the security characteristics and state of all devices on a corporate network. Categorise and assess them for vulnerabilities, and remove any that deviate from security policies," he says.

In a similar vein, Walmsley at Vectra says that a good IT team and security team "will be good business partners of the wider business". That means being facilitators where possible and not, as he puts it, becoming "the department of 'no'".

A CISO'S GUIDE TO PROTECTING THE ORGANISATION DURING OVID-19

ROSS MCKERCHAR, CISO, SOPHOS, SHARES TOP TIPS ON HOW IT AND SECURITY LEADERS CAN MITIGATE THE CYBER RISKS BROUGHT BY WORKING REMOTELY.

> yber-attackers are resourceful and opportunistic. They will move quickly to take advantage of a situation. COVID-19 is no different.

There is a huge amount of global uncertainty and change right now which criminals are seeking to capitalise on. The risks are amplified by the immediate and unforeseen IT challenges that companies are having ensuring their staff can work from home.

There are two areas which are most likely to result in a cybersecurity incident due to the ongoing crisis: remote access and phishing. Below is a set of prioritised recommendations to prevent, or at least mitigate, these issues.

Remote access

This refers to the myriad ways organisations are allowing their employees to work from home. These range from the obvious "traditional" remote access services, such as VPN and terminal service gateways, as well as cloud-native conferencing and other collaboration tools that organisations everywhere are adopting.

The key risk is weak authentication of your remote access services.

Organisations have been battling for years to ensure services (particularly when internet-facing) are protected by multi-factor authentication (MFA) and only accessible with centrally-managed corporate accounts (typically held in Active Directory, Azure or Okta).

The security problems occur for a couple of reasons. Firstly, changes being made guickly on the front line may not been seen or understood by leaders in the organisation better placed to evaluate the resultant risk. Secondly, even when risk assessments were made, the original premises are probably no longer correct.

What should IT and security leaders do?

There are long-term and short-term fixes. Long-terms fixes boil down to a zero-trust approach. There is no doubt

"STAY VIGILANT. CORONAVIRUS-RELATED ATTACKS WILL LIKELY RAMP-UP OVER THE COMING WEEKS AND MONTHS."



this crisis will accelerate the shift towards zero trust architectures.

Organisations should focus their efforts on tactically reducing risk as quickly as possible. Primarily this means ensuring key services as protected with MFA by any means possible.

This is best tackled per service. Organisations need to identify which services are most at risk and most valuable to their adversaries. For organisations with on premise infrastructure and traditional perimeterbased security these are likely to be VPNs and other remote access gateways.

For organisations with cloud infrastructure, the focus should be their identity provider (most commonly Azure or Okta). As the central point for authentication, simply enabling MFA here will get you the biggest and quickest win, especially as both Azure and Okta have integrated MFA capabilities and integrations with popular 3rd party providers such as Duo.

Making tough trade-offs

Even these tactical options are not easy and compromises will need to be made. The exact balance of trade-offs will be different for every organisation but here are some considerations:

VPN Capacity

If you're backhauling client traffic to scrub, allowing "Split VPNs" (where

clients go direct to the internet) is the quickest way to gain capacity and likely less risky than exposing squishy, insecure internal services directly online.

However, this does depend on your clients having well-patched browsers and, ideally, endpoint based web-protection. Also be aware that if you have SaaS services relying on clients coming from known corporate IP addresses don't simply turn off that control – replace it with MFA!

Centralised vs de-centralised MFA

Attaching MFA to your identity provider allows for a common experience across all applications. This is undoubtedly less confusing for staff and easier to rollout. It's also a much longer route if you don't have a centralised identity service.

"ORGANISATIONS SHOULD FOCUS THEIR EFFORTS ON TACTICALLY REDUCING RISK AS QUICKLY AS POSSIBLE."

SMS-based MFA

There's a lot of very valid concerns about SMS-based MFA. It's also the simplest and quickest way to get MFA enabled, particularly as staff will likely be familiar with it.

Passwords

If you're spinning up new services (e.g. video-conferencing) and are unable to setup federated identity, employees are going to need to remember even more passwords. The biggest risk with this is password reuse.

You can't reasonably expect employees to remember dozens of unique passwords. A password manager is the best tool to get around this problem.

OTHER CONSIDERATIONS

Beyond MFA there are a couple other

related remote-access risks to consider:

VPN and Remote access gateway vulnerabilities

Patching critical infrastructure probably feels risky right now. Unfortunately in the past few months there have been some very serious vulnerabilities in common remote access equipment.

If you have a vulnerable service you need to patch immediately. Just have a backup plan in-case the device fails to patch.

Endpoint security updates

Check your infrastructure to make sure that you are still receiving updates from your endpoint security provider. If you have a cloud-based management you're probably ok but if not, it's essential that your clients can reach updating services.

This requires checking that your VPN allows access to your update server(s) (and that you have capacity).

Phishing attacks

Phishing attacks using COVID-19 as a lure are the most visible and immediate cybersecurity risk in the ongoing crisis.

Firstly, everyone is worried and handling an unprecedented change to their daily lives. High stress situations make everyone hungry for information and less likely to objectively evaluate any message they receive. Secondly, IT departments and service providers are bombarding us all with legitimate messages about changes to services.

Combine these issues and it's unrealistic to expect employees to accurately identify and report all attacks. You need to assume that some will get through and some staff will be duped.

Accepting this allows you to focus on being resilient to attacks rather than hoping to avoid them.

MFA

Credential phishing, whereby the attackers put up a fake login page to trick

staff into entering their credentials, is the most common form of phishing. MFA is a great form of defense against this.

Awareness

By encouraging phishing reports from staff you can warn others, and if you have a security operations team (or service), even analyse the attack to identify indicators or compromise to feed into threat hunting processes.

Endpoint and email defences

Your security software has multiple chances at catching a phishing attack. The more chances you give it the better the overall protection:

- It can refuse to even receive the email as it knows it's coming from spammer.
- It can scan the email and all the attachments and URLs in order to block it.
- Web filtering can block connections to malicious websites or spot a malicious payload on the site.
- Endpoint software can spot malicious files and behaviour should all the previous defenses fail and the employee ends up running something malicious on their system.

The better-configured and effective all these defenses are the less likely an attacker will manage to evade everything.

Patching

Drive-by-downloads are less common nowadays but still a real risk. Patching browsers, mail clients and applications (such as Microsoft Office) which are regularly used to open attachments will limit the really nasty attacks that rely on minimal user-interaction.

Lastly, there are few reasons to be running browser plugins such as Flash, Java, etc. nowadays – disable them if you possibly can, it's much easier and safer than trying to keep them update.

Stay vigilant. Coronavirus-related attacks will likely ramp-up over the coming weeks and months. 1

DEFENDING DATA



DATA, SIMPLY PUT, IS BECOMING THE MOST VALUABLE, YET MOST VULNERABLE ASSET FOR ANY ORGANISATION. **SAM EMMANUEL**, BUSINESS UNIT MANAGER, GULF IT, SHARES INSIGHTS INTO THE EVOLUTION OF DATA PRIVACY AND SECURITY STRATEGIES.

> hat a comm orgar when priva

hat are the most common missteps organisations take when it comes to data privacy?

Data privacy is a multi-facetted approach that organisations need to take to protect their data in corporate environments. A majority of today's enterprises lack awareness towards this because traditionally they are used to looking at data security as a solution rather than an approach. The primary reason behind this is the change in the way data is being accessed across various datastores. Many organisations are adopting new methods to keep up with growing business needs, many of these procedures are dictated by the transformation in their approach to security as well. They need to understand that unless we keep up with the trends, we will always be catching up with the bad guys. Data security is not a one-off configuration but a constantly evolving strategy.

How can they implement strong data protection measures without sacrificing productivity in the workplace?

The success of any security strategy requires the involvement of all stakeholders within the organisation. Implementing data security in complex customer environments requires an active communication channel and we ensure that our customers understand this to ensure that they yield maximum returns. Implementing workshops around data security will go a long way in helping business and technical stakeholders to understand the critical pain points and in ensuring productivity is not hampered in the process.

What kinds of technologies and initiatives should organisations invest in to bolster data privacy measures within their organisations?

The first step towards fixing a problem is identifying the existence of one. Human error is the biggest reason for breaches and exposure. This points us towards the direction of minimising the impact of this element from the chain. Organisations need to take steps to ensure that there is a level of automation in the chain of command and that users are compliant. Solutions such as information rights management, configuration management tools, vulnerability management and application security

"DATA SECURITY IS NOT A ONE-OFF CONFIGURATION BUT A ← CONSTANTLY EVOLVING STRATEGY."

are some of the essential solutions required. These tools help in setting the foundations of security strategies and maintaining uniformity of the security posture.

How has GDPR impacted regional businesses after it was implemented in May 2018? Do organisations in the region have a better understanding of this regulation now?

GDPR was a defining point in the information security world because of its global implications. I feel even though we knew it coming, the preparations weren't ideal, and people are still just catching up to it even today. Understanding about 160 requirements of GDPR has been a significant challenge for many businesses, especially with the local market dynamics.

Since the enforcement of the GDPR penalties is being delayed, people are still trying to comprehend the finer implications to ensure they meet the legal and technical requirements. We are trying to spread the awareness among the customers to ensure that their data security polices include the GDPR regulations as well.

Are the existing regulations aimed at data protection and privacy enough? If not, what do you think is lacking the regulatory space?

The current data protection frameworks and regulations are designed to address the major security gaps in most enterprises. But every organisations' risk for data exposure differ depending on their business requirements, hence, there is a need for customised strategies. One size does not fit all. There is a need for the technical stakeholders to be on the same page as the business owners to

"THERE IS A NEED FOR THE TECHNICAL STAKEHOLDERS TO BE ON THE SAME PAGE AS THE BUSINESS OWNERS TO DEFINE SUCH STRATEGIES TO SAFEGUARD THEIR DATA."

define such strategies to safeguard their data.

Even though the regulations address most of security gaps there needs to be a shorter revision cycle for the regulations to keep up with the speed of changing cybersecurity space keeping in mind the trend of the breaches that have been taking place.

As an IT security distributor, how is Gulf IT promoting the importance of data privacy within enterprises? What kinds of offerings do you have in this space?

Gulf IT has been a pioneer in the VAD space in the region. For us, it has never been about the product but about the data security strategy. The customer preference for Gulf IT is primarily due to the problem-solving skills we bring to the table for them through the best-of-breed technologies. Our focus has been on working with vendors that add a value to customer environments. We work with Imperva, Seclore, NNT and Sailpoint within our data security portfolio. They've always believed in Gulf IT's approach of trying to help customer environment to have a holistic view of the of structured and unstructured data security. They have proven time and again on how an effectively implemented solution can help customers achieve their intended goals without compromises 指

INGRAM





Power up your business with Dell EMC PowerEdge servers

Combine our industry-leading¹ servers with your own trusted expertise, and you can open up new opportunities for your own business while helping customers to modernize theirs.

Explore the potential of advanced Dell EMC PowerEdge servers – powered by the latest Intel® Xeon® processors – to transform your business...

Z

Scalable Business Architecture Explore the latest PowerEdge portfolio powered by Intel[®], and you'll discover loads of innovative features that will help you build your business while you help your customers optimize their IT operations:

200

Intelligent Automation

For more information please visit www.ingramdellemc.com

Ingram Micro Innovation Hub | Dubai Internet City - UAE | P.O.BOX: 33550 Tel: +9714 3697111 | Fax: +9714 3697110 Website: ae.ingrammicro.com



Integrated Security

6 CRITICAL ATTACK6 CRITICAL ATTACK8 CRITICAL ATTACK

FOR MANY BUSINESSES, THE DATA CENTRE IS SEEN AS A STRATEGIC ASSET IN THEIR EFFORTS TO SUPPORT BUSINESS ACCELERATION REQUIREMENTS. **MATT WALMSLEY,** EMEA DIRECTOR, VECTRA, GIVES US A LOWDOWN OF THE MOST CRITICAL ATTACK VECTORS THAT THREAT ACTORS ARE USING AGAINST DATA CENTRES.

ata centres, and the wealth of information they contain, represent a tantalising prize for attackers. But unless the attacker gets lucky and finds an Internet-facing vulnerability, directly compromising a data centre takes a significant amount of effort and planning.

As a result, cyber-attacks that target data centres tend to be patient, mature operations that emphasise persistence and require flying below the radar of security teams. From our experience, here are the six most critical attack vectors and techniques that sophisticated cyber attackers use against data centres.

Co-opting administrative access

Administrators have unparalleled access

to the data centre and as a result are natural targets for attackers. Administrative protocols can give attackers backdoor access into the data centre without the need to directly exploit an application vulnerability. And by using standard admin tools such as SSH, Telnet or RDP, attackers can easily blend in with normal admin traffic.

Closing the local authentication loophole

In addition to the standard paths utilised by administrators, many data centres rely on local authentication options, that can be used in an emergency, to access the hosts and workloads they need to manage. However, these local authentication options are not logged, and the same login credentials are often

Matt Walmsley, Vectra

> shared across hosts and workloads for the sake of simplicity. When attackers find the credentials by compromising an administrator, they can silently access the data centre without fear of their activity being logged.

The administrative hardware backdoor

Local authentication offers an example of a backdoor that administrators — and attackers — can use to gain access to a data centre. However, there are other examples that take the same approach and extend it deeper into the hardware.

While the data centre is synonymous with virtualisation, the virtualised environments and resources still need to run on physical hardware. Virtual disks are ultimately dependent on physical disks, and the physical disks run in physical servers. Physical servers likewise have their own management planes designed for lights-out and outof-band management. The management planes have their own management planes have their own management protocols, power, processors, and memory, which allow admins to mount disks and re-image servers even when the main server is powered off.

These actions are often performed via protocols such as the Intelligent Platform Management Interface (IPMI). While many hardware vendors have their own branded versions of IPMI — such as Dell iDRAC or HPE Integrated Lights-Out (ILO) — they are all based on IPMI and perform the same functions.

IPMI and its related protocols have well-documented security weaknesses and are often slow to receive updates and fixes. Additionally, there is currently a worrying 92,400 hosts' IPMI interfaces exposed to the internet. The combination of IPMI vulnerabilities and its immense power make it a major attack vector for bad actors that are trying to subvert the security of the data centre.

Advanced attackers aim low

Unfortunately, hardware problems in the data centre don't end with IPMI. Advanced attackers, including nationstates, increasingly target physical servers, routers, switches, and even firewalls. At a fundamental level the attackers use rootkits that sit below the level of the operating system, making them extremely difficult to detect using traditional methods.

"THE MOST COVETED STOLEN ASSET FOR AN ATTACKER IS ADMINISTRATOR CREDENTIALS BECAUSE THEY ENSURE NEAR AUTONOMY INSIDE THE VICTIM'S NETWORK."

These techniques allow attackers to infect the very devices that are trusted and charged with protecting the network, and then use those devices to launch attacks deeper into the network.

Keeping an eye on data

The ultimate goal of most attacks is to steal data. Depending on their needs and skill level, attackers can use a variety of approaches to smuggle data out of the data centre. The most obvious approach involves moving data in bulk out of the data centre, either directly to the Internet or to an intermediate staging area in the campus network.

Subtle attackers may attempt to stay low-and-slow by patiently exfiltrating data at rates that are less likely to be noticed or arouse suspicion. Efforts can also be made to obscure data exfiltration in hidden tunnels within normally allowed traffic, such as HTTP, HTTPS or DNS traffic.

Blending physical and virtual context

Data centres are unique to their own organisations and vary based on applications and how users interact with them. The most common type of data centre today is the private enterprise data centre. Attacks against these data centres are typically extensions of attacks against the larger enterprise.

For example, attackers may have

initially compromised an employee laptop via a phishing email or social engineering. Next, attackers typically look to establish persistence within the network by spreading from the initial victim to other hosts or devices. To control the ongoing attack, attackers will plant backdoors or hidden tunnels to communicate back and forth from inside the network. Over time, attackers will map out the internal network, identify valuable resources, and compromise devices and user credentials along the way.

The most coveted stolen asset for an attacker is administrator credentials because they ensure near autonomy inside the victim's network. Administrator credentials are particularly essential for data centre attacks, since administrators are often the only individuals who can access data en masse.

The key point is that an attack is typically at a mature stage by the time it reaches a private data centre. The hidden command-and-control traffic, the reconnaissance, the lateral movement and the compromise of user and admin credentials are all prerequisites that lead up to the intrusion into the data centre.

Conclusion

While most data centre security has focused on protecting the virtualised layers of the data centre and microsegmentation, real-world attackers are increasingly subverting the physical infrastructure that the data centre depends on.

The use of advanced attacker detection models that expose hidden attacks against application, data and virtualisation layers in the data centre, as well as the underlying physical infrastructure, will enable security teams to address critical vulnerabilities at every layer of the virtualised data centre, even when attackers use legitimate services and protocols for their illegitimate actions. **1**





Future-Proof Connectivity Solutions



COPPER



FIBER





FTTH

RACKS

Optimize your ICT infrastructure with D-Link innovative, yet reliable Structured Cabling Solutions

www.dlinkmea.com



SMART ACCESS FOR SECURE CONTROL



SECNOR ACCESS CONTROL SYSTEM

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.





Norden Communication UK Ltd

Unit 13, Baker Close, Oakwood Business Park, Clacton-on-Sea, Essex, C015 4BD, United Kingdom Tel: +44 [0] 1255 474063, E-mail: support@norden.co.uk, Web: www.norden.co.uk www.nordencommunication.com