SENTARIS MONTHLY BRIEFING

MAY 2020

INSIDE THIS ISSUE

FOREWORD BY OUR MANAGING DIRECTOR

JUSTIN WAITE

COVID-19 has been a testing time for almost all organisations in different ways requiring many to adapt through rapid innovation and development. However, it is not only businesses that have innovated during these times, but cybercriminals have also seen many opportunities to exploit the new weaknesses that our current climate has presented. Security assurance and governance of technology have taken a back seat for many companies over the past few months as the scramble to deploy solutions. However, it is not too late to revisit those solutions to ensure they have not introduced an unexpected risk to the organisation.

Sentaris

COVID19 CYBERSECURITY BUDGET CONSIDERATIONS

JUSTIN WAITE, SENTARIS

Covid-19 has forced many organisations into using technology in ways they never expected. Staff may be working at home, with the need to access the company's system remotely. Or, organisations may have established online platforms for customer engagement with very little planning and preparation.

These rapid innovations can open up many exciting opportunities for your company. Unfortunately, Sentaris has also seen an increase in the compromise of IT systems as a result of the urgent need for organisations to go online. These compromises range from fraud, to the theft of customer information, through to poorly configured servers as well as poorly written web applications.

As we approach the start of the new financial year, ***Sentaris recommends expanding your security budget to ensure that recent innovation and decisions around technology have not introduced any exposures.*** Here are some cybersecurity suggestions that your organisation may wish to consider adding to its FY21 budget. Implementing these methods, among others, will help put your company on solid ground as you face the opportunities and challenges that Covid-19 brings.

STAFF AWARENESS TRAINING

Prioritise cybersecurity awareness training for staff members, including a mock phishing attack. This will ensure that employees stay vigilant while working from home. For maximum effectiveness, mock phishing exercises should mimic the technologies used by your organisation.

REVIEW ANY INNOVATIONS FOR SECURITY WEAKNESSES

***Implement a security design review and Penetration Test*.** This review should include public-facing websites, remote access solutions, and any other solutions that were established during the Covid-19 lockdown.

DEVICE MANAGEMENT

Ensure that all remote employees regularly update security patches and security software. Devices not connected to your organisation's network may introduce threats due to lack of security updates.

IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION

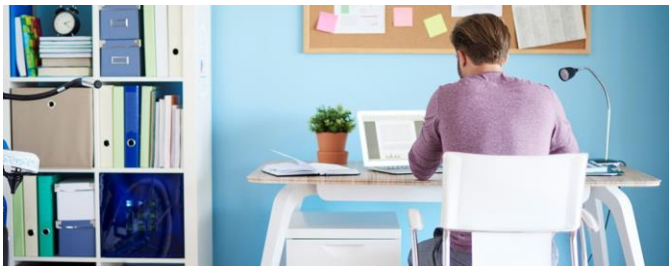
Introduce two-factor authentication for email and sensitive data. Phishing emails targeting Office 365 and Google users have been around for a long time. Now, however, the risk to remote employees is greater as they may not be protected by your company's controls.

REMOTE WORKING POLICIES

Do your employees understand what the organisation expects of them when they work from home? Organisations should ensure their working from home (WFH) and User Acceptance Policies are reviewed and updated. Many staff members will not be IT experts, so you may need to establish user-friendly ways so that remote employees use company systems securely.

If you would like assistance with any of the above cybersecurity recommendations or would like to discuss how to develop a security strategy and roadmap, feel free to contact Sentaris (https://www.sentaris.com.au/contact/).

Sentaris



MOST ORGANISATIONS NOT PREPARED TO SAFELY SUPPORT HOME

Original article by James Coker and can be found at https://www.infosecurity-magazine.com/news/organizations-prepared-safely-home/

Most organisations are not sufficiently prepared to securely support remote working even though 84% intend to continue this practice beyond COVID-19 lockdowns, according to Bitglass' *2020 Remote Workforce Report*. The survey of IT professionals found that 41% of businesses have not taken any steps to expand secure access for the remote workforce, while 65% are allowing personal devices to access managed applications.

The study was undertaken to better understand how well businesses were prepared, from a cybersecurity perspective, for the sudden surge in remote working as a result of the pandemic.

Of those surveyed, 50% said lack of proper equipment was the biggest barrier to providing secure access for employees working from home. The types of applications that organisations were most concerned about securing were file sharing (68%), web applications (47%) and video conferencing (45%).

Malware was listed as the most concerning threat vector related to remote working by IT professionals (72%), followed by unauthorised user access (59%). Unsurprisingly, anti-malware was the most utilised security tool for remote work, at 77%. However, there was a lack of deployment of tools like single sign-on (45%), data loss prevention (18%) and user and entity behaviour analytics (11%).

"This research indicates that many organisations are not implementing the security measures necessary to protect their data in the current business environment," commented Anurag Kahol, CTO of Bitglass. "For example, while respondents said that the pandemic has accelerated the migration of user workflows and applications to the cloud, most are not employing cloud security solutions like single sign-on, data loss prevention, zero trust network access or cloud access security brokers.

To continue reading, visit https://www.infosecurity-magazine.com/news/organizations-prepared-safely-home/

"This research indicates that many organisations are not implementing the security measures necessary to protect their data in the current business environment,"

IT LEADERS OVERESTIMATE STAFF'S COMMITMENT TO WFH SECURITY

Original article by James Coker and can be found at https://www.infosecurity-magazine.com/news/organizations-prepared-safely-home/

IT leaders who trust their employees to follow security best practices while working from home are sadly overoptimistic.

According to new research published today by email security firm Tessian, while 91% of IT leaders believe their staff are doing their best to work securely from home, 52% of employees believe toiling from home means they can get away with riskier behavior.

Tessian surveyed 2,000 employees across the US and the UK as well as 250 IT decision-makers to examine the state of data loss within organisations. Researchers also set out to learn how data loss is impacted by employees working remotely.

The survey revealed that 48% of employees cite “not being watched by IT” as the number one reason for not following safe data practices when working from home. The second excuse given for working on the wild side was "being distracted."

While such results might lead one to conclude that tighter controls are needed to maintain security, Tim Sadler, CEO and co-founder of Tessian, said that this tactic would not work on its own.

"Business leaders need to address security cultures and adopt advanced solutions to prevent employees from making the costly mistakes that result in data breaches and non-compliance," said Sadler.

"It’s critical these solutions do not impede employees’ productivity though. We’ve shown that people will find workarounds if security gets in the way of them doing their jobs, so data loss prevention needs to be flexible if it’s going to be effective.”

To continue reading, visit https://www.infosecurity-magazine.com/news/organizations-prepared-safely-home/

"Business leaders need to address security cultures and adopt advanced solutions to prevent employees from making the costly mistakes that result in data breaches and non-compliance,"

Sentaris

'MALWARE' TAKES AUSSIE MONEY-MANAGER MYBUDGET DOWN FOR FIVE DAYS

BILLS GOING UNPAID BY SERVICE THAT EXISTS TO PAY BILLS

Original article by Robbie Harb and can be found at
https://www.theregister.com/2020/05/14/mybudget_outage/

Adelaide-based MyBudget has been down since Saturday, 9 May. The company's client portal, app, messaging system, and its automatic payment system have all become unavailable.

MyBudget provides debt consolidation and other services for its clients, and helps them to manage money by making payments on their behalf. The company says that while the systems are down, users will not be able to access their funds and automatic payments will not be able to be processed, leaving many with urgent bills in a lurch.

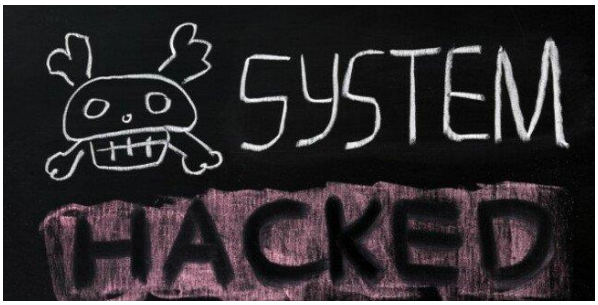
In an email to customers on Sunday, the company said it expected the issue to be resolved within 48 hours, but as of Thursday afternoon, the company's systems are still down. The company said that users can still process urgent bills over the phone, but urged them to seek extensions where possible.

The outage has led to a surge of customers calling the company to organise their finances. Users have reported being unable to get through because busy lines or very long wait times. Users took to Twitter to complain: "I have been trying all day," said @AllisonYancey. "Will my rent be paid on time this Friday or not?"

In a video update emailed to customers on Tuesday, the company's founder, Tammy Barton, assured users that their money "is absolutely safe and secure". "I want to let you know that we've been working around the clock, literally, to get everything fixed, tested and back online as soon as possible," she said.

To continue reading, visit https://www.theregister.com/2020/05/14/mybudget_outage/

Sentaris



NTT WARNS ITS SINGAPORE CLOUD WAS HACKED, JAPANESE CUSTOMER DATA COMPROMISED

EARLY MAY ATTACK HIT 600-PLUS HOSTING AND CLOUD CUSTOMERS

Original article by Simon Sharwood and can be found at https://www.theregister.com/2020/05/29/ntt_hacked_customer_breach/

As with any cyber-break-in, this one is embarrassing. But as outsourcers' whole schtick is giving clients a comfortable ride, hacks like this one belie their value proposition.

Global system integrator NTT has said someone hacked their way into its hosting and cloud services and may have accessed 600-odd customers' data.

A Japanese-language statement that *The Register* has run through a pair of online translate-o-matic services says the service provider was infiltrated on May 7 via Active Directory services running in its Singapore operations. The intrusion was confirmed on May 11. The Active Directory deployment was accessed remotely and then used internally as a stepping stone to other systems.

While a production server that ultimately came under attack was quickly triaged and the service provider quickly cut off its communications links, the hacker had managed to gain a toehold in an information management server, and reach into the company's Japanese hosting and cloud services.

621 customers of those services were then within reach of the intruder, creating "a possibility that some information was leaked due to suspicious access."

NTT said it's hardened up since learning of the hack, which it thinks was made possible by an insecure migration project. It is now working with the impacted customers and will reveal as much as it can about the attack without breaching (what remains of) its customers' confidentiality.

As with any cyber-break-in, this one is embarrassing. But as outsourcers' whole schtick is giving clients a comfortable ride, hacks like this one belie their value proposition.

Sentaris

CYBER-CRIMINALS IMPERSONATING GOOGLE TO TARGET REMOTE WORKERS

Original article by James Coker and can be found at https://www.infosecurity-magazine.com/news/cyber-criminals-impersonating/

Remote workers have been targeted by up to 65,000 Google-branded cyber-attacks during the first four months of 2020, according to a new report by Barracuda Networks. The study found that Google file sharing and storage websites were used in 65% of nearly 100,000 form-based attacks the security firm detected in this period.

The study found that Google file sharing and storage websites were used in 65% of nearly 100,000 form-based attacks

According to the analysis, a number of Google-branded sites, such as storage.googleapis.com, docs.google.com, storage.cloud.google.com and drive.google.com, were used to try and trick victims into sharing login credentials. Google-branded attacks were far in excess of those impersonating Microsoft, with the sites onedrive.live.com, sway.office.com and forms.office.com making up 13% of attacks.

Other form-based sites used by attackers included sendgrid.net (10%), mailchimp.com (4%) and formcrafts.com (2%).

Overall, the use of the Google brand by cyber-criminals to trick users appears to be increasing: Barracuda Networks observed Google-brand impersonation attacks represented 4% of all spear-phishing attacks during the first four months of 2020. This figure is expected to rise, as it has proved to be successful in the harvesting of credentials.

To continue reading, view the original article at https://www.infosecurity-magazine.com/news/cyber-criminals-impersonating/

Sentaris

IS ZERO TRUST THE BEST ANSWER TO THE COVID-19 LOCKDOWN?

ENTERPRISES NEED TO RECOGNISE THAT REMOTE ACCESS AND OTHER PANDEMIC-RELATED SECURITY CHALLENGES CANNOT BE FIXED WITH BUZZWORDS OR SILVER-BULLET SECURITY TOOLS.

Original article by Dan Blum and can be found at https://www.darkreading.com/endpoint/is-zero-trust-the-best-answer-to-the-covid-19-lockdown/a/d-id/1337785

As businesses operate under the COVID-19 shutdown, they undergo forced digitalisation. Many people are teleworking, exponentially expanding remote access loads. Organisations also experience disruption to the supply chain, business continuity/disaster recovery (BC/DR) issues, and ramped-up cyberattacks. How well they are able to navigate the new abnormal depends on where they fall in the network security continuum between a relatively closed or relatively open "zero-trust" environment.

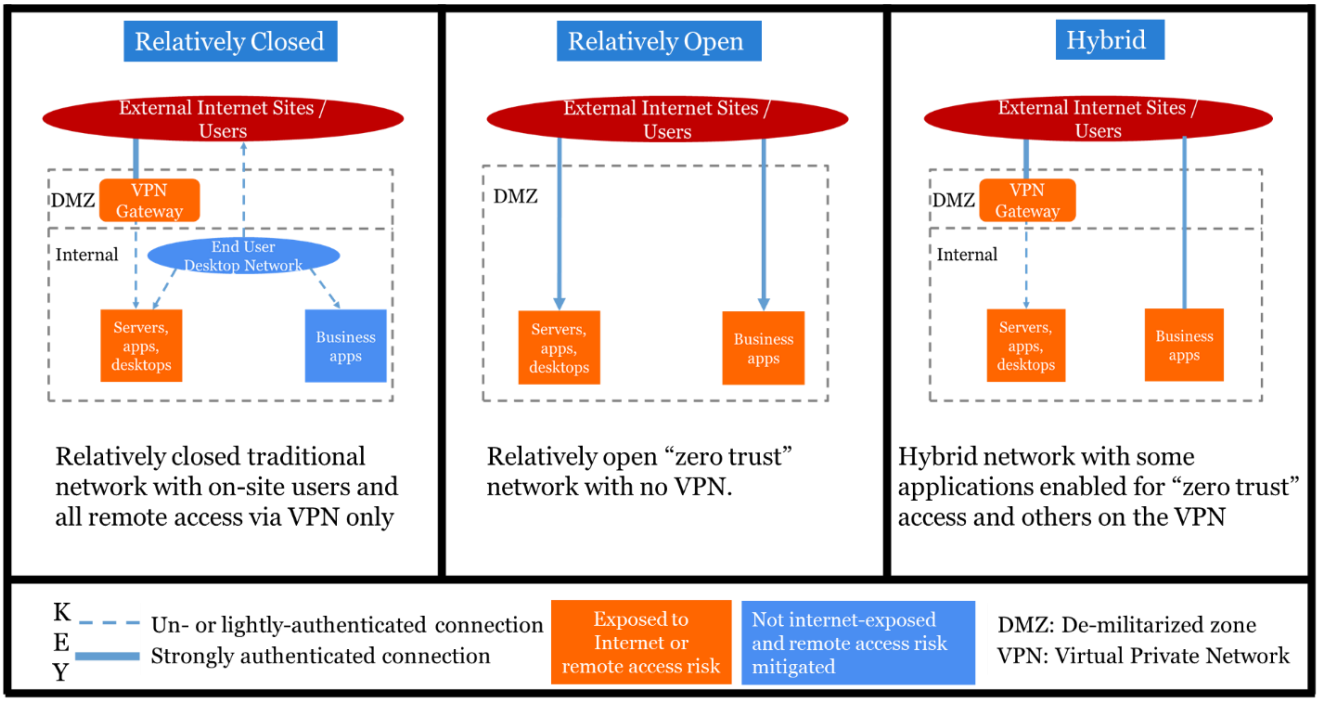


Figure 1 above illustrates three network security scenarios:

- **Relatively closed prepandemic IT environment** with main security zones of trust. Users may be strongly authenticated by the VPN, but internally to the network both users and services tend to be trusted with minimal (e.g., password-based only) authentication.
- **Relatively open IT environment** with no VPN and minimal perimeter layers. All access to applications and services gets strongly authenticated via services such as Google Authenticator or cryptographic mechanisms.
- **Hybrid environment** including elements of both the relatively open and relatively closed models.

EXPANDING REMOTE ACCESS

Businesses that had robust remote access and/or cloud security strategies before COVID-19 have found it relatively easy to ramp up teleworking. They can run many business applications as is and open up access rapidly to many others. During one of the interviews I conducted for my upcoming book, *Rational Cybersecurity for Business* — after the COVID-19 shutdown — a chief information security officer (CISO) from an asset management firm told me:

> *We'd done a tabletop exercise two and a half years ago to uncover weaknesses in remote working and fix them. This exercise was focused on the potential requirement to evacuate offices and keep the business running in the event of an active shooter scenario.*
>
> *We needed to define:*
> - *How do we communicate?*
> - *What critical systems would we need?*
>
> *Would team members have the equipment required to work at home? (We even looked at seemingly minor issues, such as whether users have headsets.)*
>
> *Architecturally, we had to make security decisions about which systems, or security zones, to keep behind the VPN and which to make accessible through the Internet. We implemented a zero-trust architecture and started to move some applications to the cloud. That really helped reduce the load on the VPN.*

Although COVID-19 has been a completely different scenario, the remote access challenges are similar. Being prepared in advance has made the disruption much less painful for us.

Although COVID-19 has been a completely different scenario, the remote access challenges are similar. Being prepared in advance has made the disruption much less painful for us.

IT'S NEVER TOO LATE, BUT…

Other businesses, whose time to prepare in advance has passed, must set themselves realistic expectations. If staff predominantly worked from the office on desktops before the lockdown, organisations may lack the budget and infrastructure capacity to swiftly roll out notebook computers to everyone. Such businesses will need to start, formalise, or expand a bring-your-own-device (BYOD) program as well as a remote access expansion project. Otherwise, they'll be opening up business applications to potentially compromised home devices. It's also important to adapt network architecture to this new way of working.

To continue reading this article, click here
https://www.darkreading.com/endpoint/is-zero-trust-the-best-answer-to-the-covid-19-lockdown/a/d-id/1337785

www.sentaris.com.au