SENTARIS MONTHLY BRIEFING

JULY 2020

INSIDE THIS ISSUE

FOREWORD BY OUR MANAGING DIRECTOR

JUSTIN WAITE

July has been a month of continued data breaches and even more critical vulnerabilities. Each month highlights the importance of ensuring organisations adopt an effective vulnerability management framework to speed up the detection and remediation of critical security risks. As seen on page 5 of this months briefing, it is not just patches that need attention but also ensuring access to critical information such as code repositories is routinely checked. We are also seeing growing evidence where breaches are occurring due to organisations only performing penetration testing during a project lifecycle, usually due to budget reasons, leaving legacy and shared services untested.

This month we have the first instalment of “Protecting your Financial Data”, in partnership with accounting firm Hamilton Morello, to help organisations understand how to protect their critical information.

Sentaris

PROTECTING YOUR FINANICAL DATA

SENTARIS IN PARTNERSHIP WITH HAMILTON MORELLO

COVID19 has forced many organisations to work differently, and as a result, there may be an increased risk to your financial data. Sentaris, in partnership with Hamilton Morello, has brought together some of the key recommendations to help you mitigate some of those risks. This first instalment focuses on general security practices, with the second instalment focusing on specific to key business practices to follow.

Article can also be viewed at ***https://www.sentaris.com.au/protecting-your-financial-data/***

General Cyber Security Recommendations

Keep it patched. Every device connected to your network, and in the cloud, should always have the latest patches applied. This means ensuring updates are installed on the operating system (such as Windows), as well as all applications installed on the device. This process should be performed regularly and is one of the best ways to protect yourself from many online threats.

Use more than just a password. You may have heard or read about 2FA (two-factor authentication) or MFA (multi-factor authentication). Think of the two factors as something that you *know* (like a password) and something you *have* (like a mobile phone, or a keyring with random numbers). This way, if for any reason your password is disclosed, cyber criminals still cannot gain access unless they also have your phone, keyring, fob, etc. This protection provides significant security over and above passwords and goes a long way to limiting the likelihood of account compromise and fraud.

Avoid untrusted networks. When accessing services containing sensitive information such as your email, accounting service, CRM etc., ensure you are only using trusted networks. It is easy to capture your passwords and other information on a network, so it is critical to ensure you never use Public Wifi (regardless of whether they are encrypted or not). As a rule of thumb: consider your home, work and tethering to your phone as more trusted. If you have no choice but to use another network, ensure that you always use a VPN first.

Turn on encryption at rest. Windows Pro has a feature called Bitlocker which encrypts your hard drive. Why is that important? If you lose your device, somebody could simply remove the hard drive from your laptop and gain direct access to all your files without needing your passwords.

AntiVirus isn't perfect, but it is mandatory. AntiVirus has come a long way and will catch a lot of malicious software, but it's not perfect. While you should never use a system without it, you shouldn't assume you are 100% protected.

“If you lose your device, somebody could simply remove the hard drive from your laptop and gain direct access to all your files”

Send links not files. Limit the duplication of financial data by storing information in a central location and only sharing the link to the file location rather than the file itself. Office 365 and Google make this process simple. Limiting data this way can avoid accidental leakage if a device is lost, stolen or compromised as additional access is required to obtain the file.

Sentaris

PROTECTING YOUR FINANICAL DATA *Cont.*

Encrypt sensitive files in transit. Ensure all email attachments containing sensitive data are encrypted/password protected with the password sent to the recipient using SMS.

Not everyone needs to see everything. Unfortunately, the natural evolution of a growing business often results in poorly configured permissions on file shares and online services where the people can have too much access. Even though you may trust everyone in your company because they all feel like family, it means attackers have more targets and opportunities to exfiltrate your critical information or make fraudulent transactions. Instead, work on the principle of least privilege and only permit access based on a persons job role. It is often easier doing this in job roles such as Management, Accounts, Marketing, Analyst etc. Assign access to data based on the groups instead of individuals, then allocate users to those groups. This makes access management more streamlined and less prone to error for when new people join, leave or change roles.

Stop trying to remember your password or writing them down! Instead, let a Password Manager auto-generate and store it for you. Password managers such as Lastpass will generate random passwords for your sites which makes them a lot more secure than "Betty12!" that you use on all your websites because it is too hard to remember OSDIFWh78@. Make sure you never use the same password twice between different applications and services. There are business versions of many password management services that provide holistic management for all employees.

Be suspicious of every email. It's not nice feeling as though you cannot trust anyone, but unfortunately, bad guys can pretend to be anyone over email, including your boss or friend. So be very careful clicking on a link or opening an attachment. If it asks you for your password, or it seems suspicious in any way, don't trust it and call the sender to ensure you can open the email.

“It's not nice feeling as though you cannot trust anyone, but unfortunately, bad guys can pretend to be anyone over email,”

Report and Review. Ensure that every month there is a reporting and review cycle to catch anomalies such as changes in employee, customer or supplier information, unusual transactions, failed logins to systems etc. Including a regular review of credit card and other bank statements to ensure small unauthorised transactions are not slipping through unnoticed.

Who are we?

Sentaris offers specialist cyber security services with a strong focus on both assurance and response. Our extensive business and specialised IT experience allows us to understand your business requirements and provide individually tailored security solutions across a broad spectrum of technologies.

Hamilton Morello has a proud history of working closely with small to medium businesses and individuals. We take the time to understand our clients' circumstances to ensure your financial growth and peace of mind. Our skilled accountants and financial planners have the knowledge to give you the right advice at the right time. With our diverse and specialised team, we offer a holistic approach to managing your finances.

Sentaris

The more cybersecurity tools an enterprise deploys, the less effective their defense is...

New research highlights how throwing money indiscriminately at security doesn't guarantee results.

Original article at https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is

The enterprise is slowly improving its response to cybersecurity incidents, but in the same breath, it is still investing in too many tools that can actually reduce the effectiveness of defense.

On Tuesday, IBM released the results of a global survey, conducted by the Ponemon Institute and featuring responses from over 3,400 security and IT staff worldwide. The research suggests that while investment and planning are on the uptake, effectiveness is not on the same incline, with response efforts hindered by complexity caused by fragmented toolsets.

The research, IBM's fifth annual Cyber Resilient Organization Report, says that while organizations are improving in cyberattack planning, detection, and response, their ability to contain an active threat has declined by 13%.

On average, enterprises deploy 45 cybersecurity-related tools on their networks. The widespread use of too many tools may contribute to an inability not only to detect, but also to defend from active attacks. Enterprises that deploy over 50 tools ranked themselves 8% lower in their ability to detect threats, and 7% lower in their defensive capabilities, than other companies employing fewer toolsets.

It does appear that the enterprise cybersecurity scene is reaching a new level of maturity, however, with 26% of respondents saying that their organizations have now adopted formal, company-wide Cyber Security Incident Response Plans (CSIRPs), an increase from 18% five years ago.

In total, however, 74% of respondents said their cybersecurity planning posture still leaves much to be desired, with no plans, ad-hoc plans, or inconsistency still a thorn in the side of IT staff. In addition, among those who have adopted a response plan, only a third have created a playbook for common attack types to watch out for during daily operations.

"Since different breeds of attack require unique response techniques, having pre-defined playbooks provides organizations with consistent and repeatable action plans for the most common attacks they are likely to face," the report notes.

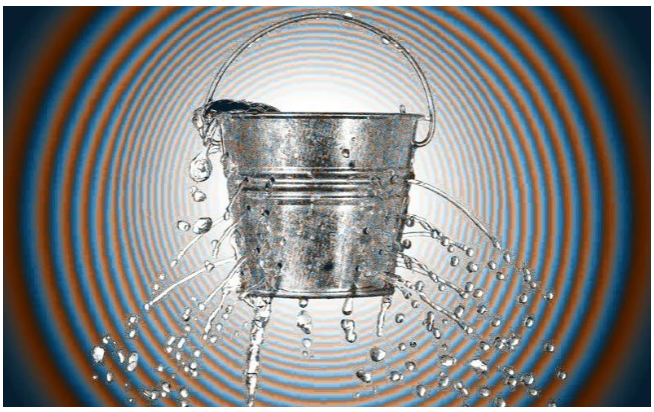
Continue reading at https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is

"In addition, among those who have adopted a response plan, only a third have created a playbook for common attack types to watch out for during daily operations."

Sentaris can help you create your incident response plans and playbooks

Sentaris

Source code from dozens of companies leaked online



Original article can be found at https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/

Source code from exposed repositories of dozens of companies across various fields of activity (tech, finance, retail, food, eCommerce, manufacturing) is publicly available as a result of misconfigurations in their infrastructure.

A public repository of leaked code includes big names like Microsoft, Adobe, Lenovo, AMD, Qualcomm, Motorola, Hisilicon (owned by Huawei), Mediatek, GE Appliances, Nintendo, Roblox, Disney, Johnson Controls; and the list keeps growing.

Operation 'Confidential & Proprietary'

The leaks have been collected by Tillie Kottmann, a developer and reverse engineer, from various sources and from their own hunting for misconfigured devops tools that offer access to source code.

A large number of these leaks, which go by the name “exconfidential” or the more tongue-in-cheek label “Confidential & Proprietary,” are available in a public repository on GitLab

According to Bank Security, a researcher focused on banking threats and fraud, code from more than 50 companies is published in the repository. Not all folders are populated, though, but the researcher says that credentials are present in some cases.

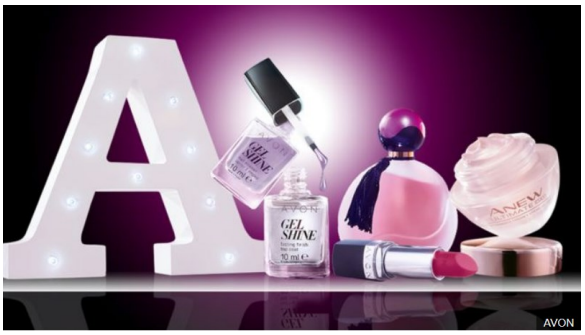
Kottmann’s server shows code from fintech companies (Fiserv, Buczy Payments, Mercury Trade Finance Solutions), banks (Banca Nazionale del Lavoro), developers of identity and access management (Pirean Access: One) and games.

Kottmann told BleepingComputer that they find hardcoded credentials in the easily-accessible code repositories, which they try to remove as best as they can, to prevent direct harm and avoid contributing in any way to a larger breach.

Sentaris recommends to routinely check all code repositories for weaknesses. This should be part of your monthly vulnerability management lifecycle.

Continue reading at https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/

Sentaris



Cybersecurity vulnerability at major cosmetics brand leads to 7 gigabytes+ data leak

The following are snippets from the original article at https://www.safetydetectives.com/blog/avon-leak-report/

One of the world's well-known cosmetic brands has been informed that a significant data breach was discovered on its web server, which was found to be publicly exposed, without password protection or encryption.

In a statement to the market on 9 June 2020, Avon put out a statement confirming that an incident had "interrupted some systems and partially affected operations"; indicating that the statement was referencing a different issue that may, or may not, be related to the breach discovered by our security team.

A few days later, Avon submitted a second regulatory filing declaring that no financial data was involved "as its main e-commerce website does not store that information". The company has also confirmed that its various online operations around the world remain in various stages of recovery, with some regions operating normally while others, still offline.

Avon.com's server contained API logs for the company's web and mobile sites which meant the data breach exposed all production server information including internal "OAuth tokens".

Similar to access tokens, OAuth tokens are used for sign-in purposes, with the key difference being that they expire after a limited time. Therefore, users must generate refresh tokens to obtain a new OAuth token. In the case of Avon.com's server vulnerability, both the sign-in and refresh tokens were exposed which is sufficient for malicious hackers to obtain full access to an account.

From index logs, our security team was able to find the following tallies:

- More than 665,000 technical log entries, including token values and internal resources such as APIs,
- Almost 3 million technical log entries and errors including private/sensitive information such as login PIN codes sent by SMS, date of birth and phone numbers,
- 11,000+ entries marked as "salesLeadMap", showing values such as full names, addresses, account settings, dates of birth, token values, last payment amounts and GPS coordinates,
- Approximately 780,000 technical log entries exposing potentially sensitive technical information, such as administrator user emails and what seems to be a list of admin system permission categories,
- Close to 450,000 technical log entries and application/Java errors, potentially exposing sensitive technical information about the server.

This kind of exposure is often missed when Penetration Testing is restricted only to specific projects and deployments.

Ensure you conduct annual penetration testing and/or perimeter scanning across all internet accessible hosts.

Sentaris

Average Cost of a Data Breach: $3.86 Million

New IBM study shows that security system complexity and cloud migration can amplify breach costs.

Original article can be found at https://www.darkreading.com/attacks-breaches/average-cost-of-a-data-breach-$386-million

The latest edition of IBM's annual cost-of-a data-breach study shows that security system complexity and incident response testing are two factors that have the biggest impact on the total cost of a breach.

The 2020 IBM study — conducted by the Ponemon Institute — is based on data gathered from executives at 524 organizations around the world that experienced a data breach between August 2019 and April 2020. For purposes of the study, Ponemon only considered data breaches that involved between 3,400 and 99,730 compromised records.

To calculate how much a breach might have ended costing a company, the research considered the costs associated with four process-related activities: the costs involved in detecting a breach, including investigation and forensics activities, assessment and audit; notification costs; lost business from system downtime and disruption and; legal fees and costs related to activities like providing help desk services, credit monitoring, and ID protection for victims.

The analysis showed that globally, a data breach cost companies $3.86 million per incident during the nine-month period of the study. The average breach cost in the US as usual was more than twice that, at $8.64 million on average. Healthcare organizations globally once again shelled out more on average for a data breach — $7.13 million — than organizations in any other sector.

Even though breach-related costs increased for many organizations, the global average of $3.86 million itself was marginally lower than the $3.92 million reported last year. That was because there were more organizations in the 2020 study with mature security practices, and therefore substantially lower breach costs, compared to 2019.

The IBM/Ponemon study showed that total data breach costs for organizations that reported having a complex security system environment was nearly $292,000 higher on average than companies that did not have the same issue. Other factors that substantially amplified the average cost of a breach included cloud migration ($267,469), security skills shortages ($257,429), and compliance failures ($255,626).

Continue reading at https://www.darkreading.com/attacks-breaches/average-cost-of-a-data-breach-$386-million

The financial impact of breaches could be minimised through more proactive identification of risks through penetration testing, and faster response through embedded Incident Response Plans and Playbooks.

Sentaris

JULY VULNERABILITY ROUND UP

BY JUSTIN WAITE

This month we have seen more remote code execution vulnerabilities which should be patched as a matter of priority. The following vulnerabilities are some of the more critical vulnerabilities that require immediate attention:

Critical Magento Flaws Allow Code Execution

Adobe has released patches for critical and important-severity flaws in its popular Magento e-commerce platform. Critical flaws in Adobe's Magento e-commerce platform – which is commonly targeted by attackers like the Magecart cybergang – could enable arbitrary code execution on affected systems. https://threatpost.com/critical-magento-flaws-code-execution/157840/

Critical SAP Recon flaw exposes thousands of customers to attacks

SAP patched a critical vulnerability affecting over 40,000 customers and found in the SAP NetWeaver AS JAVA (LM Configuration Wizard) versions 7.30 to 7.50, a core component of several solutions and products deployed in most SAP environments.

The RECON (short for Remotely Exploitable Code On NetWeaver) vulnerability is rated with a maximum CVSS score of 10 out of 10 and can be exploited remotely by unauthenticated attackers to fully compromise unpatched SAP systems according to Onapsis, the company that found and responsibly disclosed RECON to the SAP Security Response Team. https://www.bleepingcomputer.com/news/security/critical-sap-recon-flaw-exposes-thousands-of-customers-to-attacks/

Vulnerability in Windows Domain Name System (DNS) Server

Today we released an update for CVE-2020-1350, a Critical Remote Code Execution (RCE) vulnerability in Windows DNS Server that is classified as a 'wormable' vulnerability and has a CVSS base score of 10.0. This issue results from a flaw in Microsoft's DNS server role implementation and affects all Windows Server versions. Non-Microsoft DNS Servers are not affected. https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/

Sentaris


Sentaris
“Setting a new standard in Penetration Testing and Security Services”