BDO NEWS

October 2020

www.bdo.com.hk

TECHNOLOGY UPDATES
October 2020 Issue

CONTENTS

Innovation and technology are drivers for organisation growth and the key to enhance competitiveness of different industries. Just as technology rapidly evolves, so does the sector. In every monthly issue of our 'Technology Updates', it will include the latest updates from cybersecurity, emerging technology & data privacy.

Email provider was hacked and the importance of independent review over IT services providers

Many companies nowadays outsourced their email system to third parties, Software-as-a-Service (SaaS) vendors, in order to reduce costs and focus on achieving primary business goals. However, are these IT vendors secured enough to protect your companies against IT security threats? In April 2020, an Italian email provider Email.it confirmed having the security breach to the ZDNet. According to the ZDNet news, more than 600,000 users' data has been compromised.

Companies that are using Email.it may not have verified whether the Email.it has security and privacy controls in place. When email system was hacked in January 2018, the data of these companies using Email.it service between 2007 and 2020 were exposed. Those data included plaintext passwords, email content, and email attachments.

Apart from security breach, since Email.it is an Italy company, the company may provide email service to other companies that handling European personal data. In this regard, we believe the security incident may be subject to penalty if violating General Data Protection Regulation (GDPR).

A comprehensive IT security review for IT vendor is necessary because the security review helps companies understanding and thereafter manage the risks posed by

vendors. If those companies commission a service organisation control (SOC) reporting through independent third-party auditors, they would choose email service providers that has met SOC 2 and SOC 3 reporting standards to protect the privacy of their email system.

Why should companies care about the IT vendor security risks?

Nowadays, many companies only focus on their own system security, but neglect the efforts of its third-party vendors. However, does the IT vendor provide secure systems? According to the eSentire survey conducted in 2019, they found that 44% of the surveyed firms had experienced significant data breaches caused by third-party vendors. In short, since IT vendor may fail to safeguard systems against IT security threats, companies should consider vendors' security level when managing IT security.

However, it is difficult, if not impossible, for companies to physically visit the vendors' facilities and perform professional IT review over vendors' security controls. The service organisation controls (SOC) report aids this process. Companies should commission independent assessors to prepare SOC reports for verifying vendors' control implementation.

What is the service organisation controls (SOC) report?

Established by the American Institute of Certified Public Accountants (AICPA), the SOC report is an auditing report performed by certified public accountant (CPA) firms. The SOC report enables companies to assess whether internal controls are sufficient at vendors' end.

Besides, companies should commission SOC reporting for satisfying customers' needs. Some clients, who would like to have a high-level of assurance on technology risk management, may also ask vendors for producing such report for assessment.

Read more from the sources:
https://www.zdnet.com/article/email-provider-got-hacked-data-of-600000-users-now-sold-on-the-dark-web/

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

https://www.esentire.com/blog/nearly-half-of-firms-suffer-data-breach-at-hands-of-vendors/

Successful attack on a VPN service provider

Companies may use virtual private network (VPN) to facilitate employees to work-from-home. One of the VPN service providers Pulse Secure was attacked by hackers between June and July in 2020, which resulted in data leakage of 900 companies worldwide. Once the cyber-attack has successfully granted an attacker access to proprietary company data, subsequent attacks of spoofing, tampering, or privilege escalation can be initiated.

How does virtual private network (VPN) facilitate secure communication?

VPN is useful for secure remote access network between multiple systems. VPN protects data in transit by tunneling, meaning the encryption of sensitive traffic, so as to prevent sensitive information from viewing by network sniffers. As a result, applying VPN enables remote user to securely connect to the main system in order to sustain business operations remotely.

Is using VPN a secured solution?

There is no completed secured solution in the world and VPN has no exceptions. Additionally, even if the companies apply technology solutions from large service providers, they are not 100% secured.

Even if your company acquires the best VPN service, the data security may still be insecure due to lacking of comprehensive security controls. Those examples are allowing weak passwords for the email system, using insecure encryption algorithm for data in transit and not deploying security patches timely. These create severe security loopholes.

As a result, the unprepared IT infrastructure can be vulnerable, favoring cybercriminals to launch cyber-attacks. For instance, the world's leading technology company in networking hardware and networking software is being found new security issues in public Common Vulnerabilities and Exposures (CVE) in its products.

We urge companies to raise awareness of the network communication risks, and promptly complete a comprehensive risk assessment and conduct a full vulnerability scan to ensure that its communication between different systems across the network are protected sufficiently.

Read more from the sources:
https://www.japantimes.co.jp/news/2020/08/25/business/authentication-data-38-japanese-firms-stolen-amid-surge-teleworkers/

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/network-security-policies-your-organization-needs-to-adopt-today

Two North American hospitality merchants were hacked in May and June

In a security alert published in the end of September 2020, the US payment processor VISA announced that their point of sales (POS) devices of two hospitality merchants were attacked in May and June this year. Hackers deployed malware

to the POS devices & stole payment card data via targeted devices.

Visa also provided details regarding how hackers unauthorised access to their merchant's network. "There is evidence suggesting that the actors employed various remote access tools and credential dumpers to gain initial access, move laterally, and deploy the malware in the POS environment", according to Visa. However, even if the malware attacks had lasted for at least two months, the merchants did not notice it prior to getting the notice from VISA's fraud disruption team. One possible reason is that the victims did not have a security operation centre (SOC) to monitor their IT environment.

What is a security operation centre (SOC) and why needed?

A security operation centre (SOC) is designed to detect and to investigate cyber threats. It monitors companies' IT infrastructure, including networks, business systems and proprietary information. The security operation centre typically includes a computer security incident response team (CSIRT), information security analysts and forensic investigators to perform cyber-attack detection.

Why is security operation centre (SOC) needed?

In the age of advanced persistent threat (APT), attacker may successfully attack your network while keeping themselves undetected for long time, not just one time. It is crucial to discover such acts continuously.

Besides, hundreds and even thousands of security events can flood companies' network every hour, every day. Your IT security team may have a significant challenge of sifting through these events to identify cyber threats that could pose a risk of compromise. However, reviewing all network activity for the entire company by IT security expertise is so resource-intensive that your IT security team may not make it or only afford regular review such as monthly or quarterly. When your security analysts review logs and discover security vulnerabilities by the regular review, hackers would have already exploited it and got unauthorised access to your mission-critical systems.

How can SOC help businesses?

A team of experts review security events, logs and network traces on a 24×7 basis can help to improve your mean-time-to-detect (MTTD). After security operation centre detects the abnormal activities, they generate alerts to your IT team promptly. Such actions also speed up your response time to contain and to minimse the risk of security breaches.

Without continuous monitoring of your network and IT systems, company may not able to identify suspicious activities efficiently and thereafter, detect and contain different cyber-attack timely. We urge companies to review their capability of detecting cyber security incidents and, if possible, apply security operation centre services.

Read more from the source:
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf

How can BDO help?

BDO Risk Advisory Services (RAS) has a team of dedicated IT professionals. We are well equipped, qualified, experienced and well-prepared to assist your board or management to perform IT security assessment, data protection review, vulnerability assessment as well as penetration test or any other IT matters relating to regulatory requirements. Please do not hesitate to contact us and talk to our consultants. We are pleased to provide further insight or assistance if needed.

BDO'S SUPPORT AND ASSISTANCE

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

RICKY CHENG
Director and Head of Risk Advisory
Tel: +852 2218 8266
rickycheng@bdo.com.hk

BDO Limited, a Hong Kong limited company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO to discuss these matters in the context of your particular circumstances. BDO, its directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

© 2020 BDO