I. Exploit on Exchange – vulnerabilities in Microsoft Exchange servers trigger a red alert

The German Federal Office for Information Security (BSI) declared a red alert – Germany’s highest alert level – in early March after it emerged that more than one hundred thousand Exchange servers had been compromised worldwide. According to estimates by the BSI’s CERT-Bund, 26,000 Exchange servers in Germany alone are vulnerable to security breaches, as acknowledged by Microsoft on 2 March this year. It has also provided security updates to patch these vulnerabilities. Until that point, these vulnerabilities were primarily exploited by the evidently pro-state Chinese hacking group HAFNIUM, for whom the exploits were named. Then, on 10 March, a security researcher tweeted that he had found a similar exploit that would have allowed him to hijack Exchange servers. The European Banking Authority (EBA) was one of the most high-profile victims of the global wave of attacks. Although it had to take its mail servers offline after the attack, it managed to resume email communication on 9 March.
Cybersecurity authorities like the BSI believe that HAFNIUM wasn’t the only group to seize the opportunity; they assume that other cybercriminals also swooped in swiftly and successfully compromised Exchange servers before the updates had been applied. They are worried that a huge wave of ransomware will arise because, according to their findings, the hackers have installed well-concealed back doors on all accessible or networked servers that they will use at a later time for classic extortion attempts. We’ve reported repeatedly in recent issues about the impact that Trickbot and other ransomware has had on the likes of the University Hospital of Düsseldorf and on many companies, too. Another cause for concern arising from the BSI CERT-Bund’s observations is the fact that in many IT infrastructures, the Exchange servers are unnecessarily assigned very high privileges in the Active Directory. So cybercriminals will have an extremely easy time of taking over the entire system once they control access to the Exchange server.

Consequently, installing the patches that Microsoft has provided isn’t a sure-fire way of guaranteeing IT security. Instead, operators of top-priority Exchange servers are required to ensure two things:

a) First, they must check if the server is already compromised BEFORE installing the updates. If it is, they have to check how deeply the attackers have already penetrated the system.

b) Then they are supposed to install all the latest updates.

The fact that Microsoft is providing direct patches – i.e. updates that don’t necessarily require a correctly closed update chain – reflects the gravity of the situation.

While this update procedure certainly isn’t easy, it is extremely urgent and unavoidable for anyone wishing to protect their IT from potential ransomware attacks. That’s why we’re deviating from our norm by providing a source linking to all the documents that help with implementing the necessary measures in the body of this article:


On 15 April, the Swiss National Cybersecurity Centre (NCSC) announced that Microsoft had discovered and provided updates for additional vulnerabilities on 2013, 2016 and 2019 Exchange servers. The relevant links can be found on the NCSC web page mentioned below. The NCSC is also advising immediate installation of the updates in these cases.

Read more:
https://finanzbusiness.de/nachrichten/banker/article12817048.ece
https://www.reuters.com/article/us-microsoft-eba-idUSKBN281005
II. Learning by doing – data leaks discovered in the Swiss Army’s cyber training school

When compared to the huge problems and the tremendous risk potential associated with the Exchange server hack, the two data leaks discovered around the same time in Switzerland might seem rather modest. But the fact that they turned up in the Swiss Army’s learning management system, of all places, and apparently remained unresolved for an extended period before the Army moved to close them within hours made this announcement stick out like a sore thumb. What’s more, the vulnerabilities were discovered by a Swiss Army cyber trainee. He’s sure to have earned top marks for that find!

Read more:
https://www.tagesanzeiger.ch/Armee-meldet-sicherheitsluecken-bei-lernplattform-792963574253

III. Rocky start(up) at Verkada – 150,000 surveillance cameras hacked

Around 150,000 surveillance cameras and a video archive operated by US start-up Verkada were hacked in early March too – with the help of a Swiss hacktivist. ‘Advanced Persistent Threat 69420’ – an international hacker community that includes the Swiss IT specialist with the code name of Tillie Kottmann – allegedly wanted to draw attention to the systems’ widespread use and inadequate security.

The community managed to get its hands on publicly accessible data for an administrator account online and tap into the cameras with the account’s access privileges. Footage that APT 69420 leaked to Bloomberg showed ongoing operations – shots inside a Tesla warehouse, a prison and a hospital – and archive video feeds apparently stored on Verkada’s premises as opposed to its customers’ sites. The hackers also tweeted that various Verkada employees had accounts that would have granted them access to its customers’ cameras. Tillie Kottmann’s Twitter account has since been suspended, as have the aforementioned dubious administrator accounts at Verkada.

Read more:
https://www.bernerzeitung.ch/hacker-zapfen-150-000-kameras-an-tesla-spital-und-gefaeengnis-betroffen-155344967820
IV. Refunds from the remorseful Ziggy ransomware gang

In late March, bleepingcomputer.com published news that the cyber extortionists behind the Ziggy ransomware hadn’t just ceased their criminal activities, but also provided more than 900 decryption keys and a decryption tool to simplify the data liberation process. The hackers stated that their motivations in doing so were moral concerns and ever-increasing fear of prosecution. On 19 March, Ziggy’s administrator also announced that he had had a change of heart: he would refund all victims within two weeks for the ransoms they paid if they emailed proof of payment and their computer IDs to ziggyransomware@semail.pro. The refund would be made in Bitcoin at the value applicable on the day of payment. Since the cryptocurrency’s value is swiftly soaring – the price having risen 77% alone between the time the decryption keys were published and the refunds were announced – it remains to be seen whether Ziggy can afford to refund all the ransoms it extorted in full. Speaking to bleepingcomputer, the administrator claimed that the repentant extortionists would have to sell their homes to afford the refunds.

Read more:

V. Data scraping on Facebook and LinkedIn: big data brings big damage

In early January, WhatsApp announced a change in its privacy policy which would force users to share their data with Facebook – despite all the promises WhatsApp made when it was taken over by Facebook. While there was initially a huge outcry, WhatsApp’s market penetration and the fact that WeChat and TikTok had been banned by the Trump administration meant that Mark Zuckerberg’s movers and shakers could be relatively sure that there would be no major consequences for their actions. They were almost cynical in announcing this data exchange. The new privacy policy reads: ‘Respect for your privacy is coded into our DNA. Since we started WhatsApp, we’ve built our services with a set of strong privacy principles in mind.’ WhatsApp informed users that they would either have to agree to the partnership with Facebook ‘to offer experiences and integrations across Facebook’s family of apps and products’ or they would no longer be able to use WhatsApp and consequently lose all the data previously stored in their WhatsApp account.

While the uproar might have died down in the meantime, data loss has now taken on a different direction and dimension. In late March, the IT security firm Hudson Rock discovered data relating to 533 million Facebook users in a hacker forum. Although a company
spokeswoman dismissed the discovery by saying that the data came from a hack in 2019, it would be fair to assume that users don’t change their phone numbers and email addresses annually, meaning the data is still largely valid and usable.

Then, in early April, the website Cybernews reported that another social network had suffered a data leak; user data from half a billion profiles on LinkedIn (the Microsoft-owned professional networking and career platform) had been offered for sale on the darknet. Of these, 2 million were pre-released as proof, and the provider plans to auction off the rest of the package.

Given that two of the major social networks have suffered huge data leaks in just one week, astonishing parallels are emerging between the analogue and digital media worlds on the one hand, and legal and illegal marketing on the other. Facebook is already an attractive target to hackers due to the sheer size of its user base; in LinkedIn’s case, it is the quality of the users (and their data) that makes the network a prime target for attack. And it is precisely these arguments – the ‘size’ and ‘appeal’ of their readers, listeners and viewers, i.e. their users – that newspapers, magazines, radio stations and television stations have always used (and continue to use) to solicit cash inflows in the form of advertising revenue. The ‘executives and decision-makers’ target group was and is particularly attractive.

If you’d like to check whether your data was included in the hack, finding out is a fairly quick and easy process, using the ‘Have I Been Pwned?’ website, for instance. The link to the website can be found below.

Read more:
https://t3n.de/news/accounts-gehackt-passwort-adobe-pwned-514556
https://haveibeenpwned.com

This SWITCH security report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH security report discusses current topics in the field of cybersecurity. It is aimed at interested internet users and seeks to make them aware of current threats. Despite careful review, SWITCH accepts no liability for accuracy.