MA Business

network SECURITY

ISSN 1353-4858 September 2021 www.networksecuritynewsletter.com

OWASP announces new Top 10 for cyberthreats

OWASP has released details of its new Top 10 list of threat categories, with access control flaws moving into the number one spot.

The OWASP Top 10 is frequently used as guidance for risk and threat analysis, in part because it is based on extensive research. That's why it is four years since the last revision. The 2021 list, which is in draft form and open for comments, shows some highly significant changes since the 2017 version.

Injection flaws of various kinds, especially those leading to SQL injection, have remained solidly at the head of the list – until now. Broken access controls have taken its place. OWASP reports that 34 Common Weakness Enumeration (CWE) entries, "mapped to Broken Access Control had more occurrences in applications than any other category".

Examples of this kind of flaw include: allowing attackers to bypass access control checks by modifying the URL, internal application state or the HTML code on a page; allowing a primary key to be changed to another user's record; privilege escalation; and metadata manipulation.

Cryptographic failures have moved into the number two spot. This was formerly known as sensitive data exposure which, OWASP decided, is more a description of a symptom rather than a cause. The renamed category indicates a focus on the cryptographic failures that can lead to systems being compromised and sensitive information being exposed. This includes bad practices such as hard-coded passwords, insufficient entropy in passwords or keys, storing passwords without hashing and salting them, not enforcing TLS connections on web pages that require user authentication, the use of "broken or risky crypto algorithms" and so on.

The injection category is now in third place in spite of being modified to include cross-site scripting (XSS), which was a class on its own in seventh place in the 2017 list. Similarly, XML external entities (XXE) flaws have been rolled into security misconfigurations.

This has made room for new categories to enter the list. In fourth place, insecure design looks at vulnerabilities that get baked into code through poor code planning and execution. According to OWASP, security needs to be shifted further along the development process so that it is included from the very beginning. "If we genuinely want to 'move left' as an industry, it calls for more use of threat modelling, secure design patterns and principles, and reference architectures," the organisation said.

Software and data integrity failures is another new category (coming in at number eight). This absorbs the earlier insecure deserialisation category, and the new, broader class is about "making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity".

The third and final new category is server-side request forgery (SSRF), which has been added as a reaction to an industry survey undertaken by OWASP to find what weaknesses are worrying professionals even if the flaws don't yet show up in statistics such as CVEs and CWEs.

According to OWASP: "The data shows a relatively low incidence rate [for SSRF] with above-average testing coverage, along with above-average ratings for exploit and impact potential. This category represents the scenario where the industry

Continued on page 2…

Contents

NEWS

FEATURES

REGULARS

Editor: Steve Mansfield-Devine
Email: smd@contrarisk.com

Managing Director: Jon Benson
Group Content Director: Graham Johnson
Executive Director Digital Resources: Matthew Cianfarani
Subscription Director: Sally Boettcher
Circulation Manager: Chris Jones
Production Manager: Nicki McKenna
Chief Executive Officer: Ben Allen
Chairman: Mark Allen

MA Business

Part of
Mark Allen

Network Security is published
by MA Business Limited
Hawley Mill, Hawley Road,
Dartford. Kent DA2 7TJ, UK
Tel: +44 (0)1322 221144
Website: www.markallengroup.com/brands/network-security

Subscription enquiries
UK: 0800 137201
Overseas: +44 (0)1722 716997
Email: institutions@markallengroup.com
An annual subscription to *Network Security* includes 12 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

Notice
No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made. Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

Following the acquisition of Network Security by MA Business Ltd from Elsevier Limited, on 14th June 2021, MA Business Ltd is now the data controller of personal data in respect of Network Security and will process personal data in accordance with its Privacy Policy - please visit https://privacypolicy.markallengroup.com to understand how we process, use & safeguard your data and to update your contact preferences. Please note that there may be a delay with updating the website to reflect this change.

For a press release on the purchase, please visit
https://markallengroup.com/our-news/

Digitally Produced by Mayfield Press (Oxford) Limited 12987

...Continued from front page

professionals are telling us this is important, even though it's not illustrated in the data at this time."

As with earlier incarnations of the list, the OWASP Top 10 is bound to be cited in, and used as a foundation for, all manner of security activities, although OWASP is a little wary of this. It believes that the list should constitute a "bare minimum" for issues like coding standards, code review, penetration testing and tool support. In other words, it can act as a starting point, but people should be going well beyond it. Similarly, it classifies the list as "entry level" for training. And the organisation feels that it will find only occasional use in software design and architecture, unit and integration testing, and securing the supply chain. Where it is of most use, OWASP believes, is in security awareness.

There's more information here: https://owasp.org/Top10/.

US Cyber Command warns of Confluence attacks

US Cyber Command, which is responsible for the military cyber capabilities of the US, has taken the unusual step of issuing a warning to enterprises about ongoing attacks. These exploit a recently patched vulnerability in Atlassian's Confluence collaboration platform.

The flaw (CVE-2021-26084) allows for an object-graph navigation language (OGNL) injection exploit giving an attacker the ability to run arbitrary code on a Confluence server with the same privileges as the server itself. From that position, an attacker – who doesn't need to be authenticated on the service – could elevate privileges to gain complete control over the server. OGNL was also exploited in the Equifax breach in 2018, where the vulnerability (CVE-2018-11776) was in Apache Struts 2.

The flaw, which has a CVSS severity rating of 9.8 out of 10, was patched by Atlassian on August 25. But very soon after, proof-of-concept exploit code appeared online. Security company Bad Packets then reported it was seeing high levels of scanning for vulnerable systems, and other organisations confirmed similar activity.

The FBI and the US Cyber security & Infrastructure Security Agency (CISA) issued alerts, warning that malicious actors might use the Labor Day weekend in the US to launch attacks, which turned out to be the case. This was followed by US Cyber Command releasing a warning that, "Mass exploitation of Atlassian Confluence CVE-2021-26084 is ongoing and expected to accelerate. Please patch immediately if you haven't already – this cannot wait until after the weekend."

The Confluence platform is heavily used by organisations to share documents and enable collaborative working. Some of the more notable users are Audi, Docker, GoPro, Hubspot, LinkedIn, NASA, The New York Times and Twilio. The cloud version of Confluence is not affected, but many self-hosted and datacentre versions are vulnerable.

Bad Packets said it has seen threat actors in multiple countries deploying PowerShell and Linux shell scripts on vulnerable Confluence servers. Many of these attacks appear to be attempts to install crypto-currency miners, such as XMRig Monero.

One company that has fallen victim to the issue is Jenkins, an open source automation platform used by developers. Its Confluence-based service has been deprecated for the past couple of years, since when it has been read-only. Documentation and changelogs were migrated from the Confluence-based wiki to GitHub. However, the server was still reachable online and appears to have been hijacked for crypto-currency mining. The organisation said: "From there an attacker would not be able to access much of our other infrastructure. Confluence did integrate with our integrated identity system which also powers Jira, Artifactory, and numerous other services."

It added: "At this time, the Jenkins infrastructure team has permanently disabled the Confluence service, rotated privileged credentials and taken proactive measures to further reduce the scope of access across our infrastructure. We are working closely with our colleagues at the Linux Foundation and the Continuous

Threatwatch

Video vulnerability

Nozomi Networks Labs has discovered a critical remote code execution (RCE) vulnerability (CVE-2021-32941) in the web service of the Annke N48PBB network video recorder (NVR). This information has been released as part of a co-ordinated disclosure with ICS-CERT, which published advisory ICSA-21-238-02, and with the vendor, Annke, which has released firmware that fixes the issue. Exploitation of the vulnerability could result in the compromise of the device itself, as well as the data stored inside it. There's more information here: https://bit.ly/2YPr5ho.

Zloader retools

The operators of the Zloader banking trojan have retooled the malware to make it stealthier, say researchers at SentinelLabs. The malware is now being spread via ads for Microsoft TeamViewer and Zoom, as well as its usual route of Google AdWords. To reduce the chances of detection, it now uses a signed dropper. "It appears that the cyber criminals managed to obtain a valid certificate issued by Flyintellect, a software company in Brampton, Canada," the researchers explained. It also uses a backdoored version of wextract.exe, a Windows utility. These droppers are responsible for downloading the main payload. The malware is also now capable of disabling all Windows Defender modules on victim machines. There's more information here: https://bit.ly/2XlBEbb.

Fortinet flaw

Security firm Rapid7 has found a flaw in the management interface for Fortinet's FortiWeb web application firewall. If an attacker is able to authenticate on the system, it's possible to enter commands in the 'name' field of the SAML server configuration page. If these commands are surrounded by backticks, they will execute with root privileges. This could lead to an attacker installing a persistent shell, install crypto-mining software or use the platform to attack the wider network. Fortinet has patched the vulnerability, but the problem was revealed around the same time that hackers released access credentials for 87,000 Fortinet VPN devices that should have received patches two years ago. There's more information on the new flaw here: https://bit.ly/3hzcmhe.

Android banking trojan

A new Android banking trojan has been described as 'the most feature-rich Android malware on the market'. And it seems its developers have even greater ambitions for it. Dubbed Sova (Russian for 'owl'), the malware is still in its infancy, according to researchers from ThreatFabric. They say that the developers seem to be planning to add distributed denial-of-service (DDoS), man-in-the-middle (MiTM) and ransomware functionalities to the code. "Sova also stands out for being fully developed in Kotlin, a coding language supported by Android and thought by many to be the future of Android development," said ThreatFabric. There's more information here: https://bit.ly/3Ek56j2.

BlackBerry bug

BlackBerry has finally issued a critical security alert for its QNX Real-Time Operating System (RTOS), having spent four months denying that a flaw existed. QNX is used in more than 175 million cars, medical devices and industrial systems. The Software Development Platform (SDP) version 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 are afflicted with an integer overflow vulnerability in the calloc() function of the C runtime library. Tracked as CVE-2021-22156, this flaw – dubbed BadAlloc – has a CVSS severity rating of 9.0 and was originally disclosed in April 2021. It affects only older versions of BlackBerry's products. However, solutions based on these are likely to still be in widespread use. There's more information here: https://bit.ly/3huAsKL.

Delivery Foundation to ensure that infrastructure which is not directly managed by the Jenkins project is also scrutinised."

Atlassian has details, including lists of fixed and vulnerable versions of the code, here: https://bit.ly/3lj4jX1. And there are details of the proof-of-concept exploit code here: https://bit.ly/3nxbptx.

Meris botnet breaks records

A relatively new botnet has recently broken records during a month-long distributed denial of service (DDoS) attack against Russian Internet company Yandex.

Known as Meris (the Latvian word for plague), the botnet has hit other targets, too, including Cloudflare and the website of security journalist Brian Krebs.

The attack against Yandex started around a month ago but recently peaked with traffic flows of 21.8 million HTTP requests per second. This is the biggest DDoS attack ever recorded against RuNet – the name given to the segregated section of the Internet operated in Russia. This is according to Qrator Labs, a security firm that works with Yandex.

According to the Russian-language publication Vedomosti, which cited sources within Yandex, the attack was contained, but with a struggle. It said the attack was "a threat to infrastructure on a national scale". However, apart from noting the record level of traffic, the firms involved have released little in the way of details.

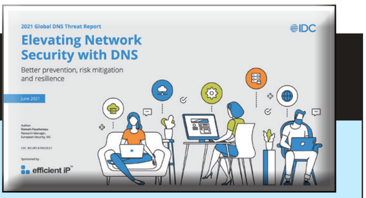
Qrator Labs said the botnet seem to be mostly routers made by Latvian firm MikroTik, the majority of which are in the US. As many as 56,000 hosts were used to attack Yandex, but some security experts, including those at Qrator Labs, have put the size of the whole botnet as high as 250,000 compromised devices.

In summer, Meris was used against Cloudflare, reaching a maximum traffic level of 17.2 million requests a second. This is nearly 70% of Cloudflare's normal traffic levels.

More recently, the botnet's operators attempted to take down Krebs' website with an attack that reached two million requests a second. In 2016, Krebs was one of the first victims of the infamous Mirai botnet. That kept his site offline for four days with an attack measuring 450,000 requests a second. The site is now protected by Google's Project Shield initiative which is why, even though the recent attack was more than four times larger, it failed to knock the site offline.

Meris appears to be exploiting port 5678 on MikroTik routers, which use that port for a neighbour discovery feature. The routers offer SOCKS4 proxy on the port which the attackers subvert with an HTTP pipelining technique. MikroTik uses UDP traffic via port 5678, but it also accepts TCP connections. A search of the public Internet by Bleeping Computer found more than 328,000 devices with 5678 open, although some of them are LinkSys products that also accept TCP on that port. Port 2000 is also open, for use in bandwidth testing. At the time of writing, MikroTik said it is not aware of its products having a flaw.

Report Analysis


2021 Global DNS Threat Report
IDC
Elevating Network Security with DNS
Better prevention, risk mitigation and resilience
June 2021
efficient IP

IDC: Elevating Network Security with DNS

The Domain Name System (DNS) is critical to the functioning of the Internet. And yet it's one of the most under-protected parts of the infrastructure. Attacks against DNS services can achieve devastating effects, from redirecting traffic to malicious sites to making whole swathes of the Internet inaccessible.

DNS servers can themselves be exploited as weapons – such as amplification techniques used in distributed denial of service (DDoS) attacks. And while efforts are in progress to strengthen the security of the DNS ecosystem – such as the implementation of DNSSEC – progress is agonisingly slow and much of the infrastructure remains vulnerable.

This survey by IDC, on behalf of EfficientIP, shows that the number of attacks in all the major categories which it tracks has increased from the previous year's report. And while exploiting DNS vulnerabilities might seem like a highly technical form of attack, it's instructive to see what those categories are and how DNS weaknesses can contribute to a number of threat areas.

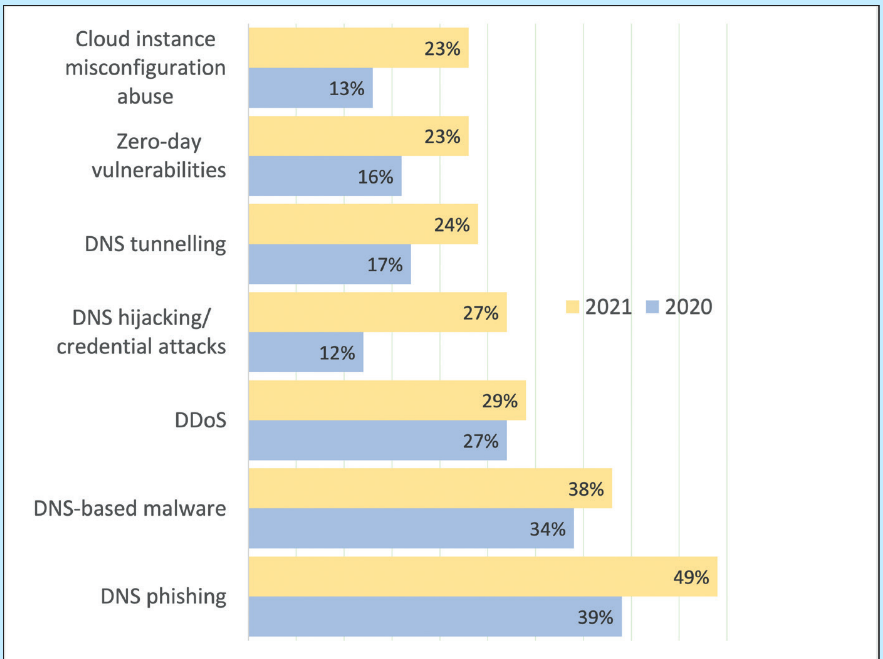
Phishing, for example, is a pernicious and ubiquitous form of attack afflicting individuals and every kind of organisation. Tricks such as DNS spoofing can play a major role by helping the malicious actors to create convincing websites that faithfully emulate legitimate sites while hosting traps for the unwary. DNS-based phishing attacks were seen by half (49%) of the organisations surveyed this year, compared to 39% the previous year, and a significant contributor to that rise has been the work-from-home trend.

The involvement of DNS in malware and DDoS attacks has risen slightly, but more significant bumps have been seen in some of the more technical areas, such as DNS tunnelling – witnessed by 24% of respondents this year compared to 17% in 2020 – and DNS hijacking and credential attacks, which more than doubled from 12% to 27%.

Overall, 87% of organisations saw DNS-related attacks this year, up from 79% the previous year. And, on average, each organisation was subject to 7.6 attacks over the course of the year. But not all industries are equally affected.

Measuring the impact of an attack isn't always a simple affair. Some of the effects suffered by firms in the past year, for example, include cloud service downtime (experienced by 46%), in-house application downtime (51%), compromised websites (42%) and brand damage (27%).

And while telecoms companies were the most frequently targeted, in terms of number of attacks, when you start breaking down the cost of attacks, the financial industry comes out as the clear leader, which isn't a good thing. The average cost of attacks across all sectors, including mitigation, lost business and so on, was $950,000. But for the financial services industry, this goes up to $1.1m – although this is actually a slight drop compared to the previous year. Some 91% of businesses in this industry suffered at least one DNS-related attack, and the average was 8.3 attacks over the year.



Percentage of organisations that witnessed the most common forms of DNS-related attacks. Source: IDC.

The financial industry is the sector most likely to experience phishing attacks (55% of organisations) and DNS-based malware (42%). Other notable DNS attack types reported were DDoS (35%), DNS tunnelling (30%), domain hijacking (30%) and zero-day vulnerabilities (26%).

"The financial industry is one that has always been of particular interest to attackers," says Norman Girard, CEO of EfficientIP. "The sector forms one important pillar of the economy and therefore damages caused here have vast consequences for many other sectors. Fortunately, the data also indicates that the industry is increasingly aware of the threat and is taking measures to improve its DNS security."

Protecting DNS infrastructure and services is becoming ever-more important, and the good news is that there's reasonably high awareness of this fact. Three-quarters of organisations contacted by the researchers acknowledged that DNS is critical to their businesses. And pretty much all (99%) claim to have some kind of DNS security in place, although how much good this is doing them is another matter.

A complicating factor is that some of the countermeasures and remediations that would be effective in the event of a DNS-related attack are seen as too disruptive to the business. These include taking down all or part of the network infrastructure, shutting down the DNS server or service and disabling applications. This reluctance is revealed in the overly long time – an average of just over 5.5hrs – it takes to remediate a DNS attack. On the plus side, 42% of organisations are now using auto-remediation systems, compared to 25% the previous year.

The report argues that, as well as protecting their DNS services, organisations should be exploiting DNS to improve their security. DNS can provide crucial support to user behaviour analysis and filtering, which in turn can build the foundation of a zero-trust framework.

The report is available here: www.efficientip.com/resources/idc-dns-threat-report-2021/.

In brief

BrakTooth affects billions of devices

Flaws in Bluetooth software stacks could leave billions of devices vulnerable to attacks ranging from denial of service or bricking through to arbitrary code execution. The issues – collectively dubbed BrakTooth – were unearthed by researchers at the Singapore University of Technology and Design. They examined 13 chipsets from 11 vendors – including Intel, Qualcomm, Zhuhai Jieli Technology and Texas Instruments – and found that they suffered from 16 previously unknown vulnerabilities, plus 20 with CVEs already assigned and four with CVEs pending. These system-on-chip (SoC) solutions are very widely deployed by device manufacturers, and so it's probable that the number of devices affected runs into the billions. "All the vulnerabilities […] can be triggered without any previous pairing or authentication," the researchers said. Three of the chipset vendors – Espressif, Infineon (Cypress), and Bluetrum Technology – have already released firmware patches, although it's uncertain to what degree these will find their way to devices already in use. There's more information here: https://bit.ly/394Vbj0.

REvil is back

The REvil (aka Sodinokibi) ransomware group appears to be back in action. The ransomware as a service operation shut down as a result of the attention it attracted when one of its affiliates attacked software firm Kaseya. That breach led to US President Joe Biden instructing intelligence agencies to investigate. It has been suggested that REvil, which operates from Russian soil, may have come under pressure from that country's Government to go underground, for a while at least. Now the group's website – the 'Happy Blog' – which it uses to leak stolen data from victims that refuse to pay, is back online, albeit showing the same information as when it went offline in July. The dark web-based payment portal through which targets pay cryptocurrency ransoms is also functioning again. At the time of writing, however, no new attacks using the REvil malware had been reported.

Mustang Panda attacks

A China-based group, tracked as Mustang Panda, appears to have infiltrated the internal networks of government ministries and agencies in Indonesia. Indonesia's main intelligence service, Badan Intelijen Negara (BIN), is one of at least 10 organisations to have had its systems compromised, according to research by Recorded Future. The researchers found that command and control servers for the PlugX malware were communicating with hosts within Indonesian government networks, and this traffic dates back to at least March 2021. It's unclear whether the attacks are state-sponsored. There's more information here: https://bit.ly/3EgyZRf.

ICS under assault

A third of industrial control system (ICS) installations were subject to some form of attempted cyber attack in the first half of 2021, according to new figures from Kaspersky. The claim is based on the firm's telemetry from its customers, which showed that it blocked more than 200,000 malware variants from more than 5,000 families. Of the 33.8% of ICS solutions targeted, 18.2% faced Internet-based threats, 5.2% were attacked by threats delivered by removable media, such as flashdrives, and 3% were hit by malicious email attachments. The figures were only a slight increase (0.4%) over the previous six months. However, Kaspersky warned that the overall, longer-term trend shows a marked increase, with a recently spotted focus on spyware. There's more information here: https://bit.ly/3lnA6WN.

First responder guide

The US National Cybersecurity Centre of Excellence (NCCoE) – part of the National Institute of Standards and Technology (NIST) – has published the final version of its 'Cybersecurity Practice Guide' for public safety first responder (PSFR) organisations, such as ambulance, fire and other emergency care operations. The guide focuses on standards-based and open-source single sign-on solutions. One of the key issues for PSFRs is solving authentication challenges so that first responders can access sensitive data quickly, without causing potentially life-threatening delays. "This practice guide describes a reference design for multifactor authentication and mobile single sign-on for native and web applications while improving interoperability among mobile platforms, applications and identity providers, regardless of the application development platform used in their construction," said the NCCoE. The guide is available here: https://bit.ly/3Acwq04.

Ransomware recovery

Just over a third of financial services firms globally were hit by ransomware in 2020. And of those, more than half (51%) had at least some data encrypted, according to research by Sophos. Its 'State of Ransomware in Financial Services 2021' report claims that 62% of affected organisations were able to restore from back-ups, but this still led to considerable recovery costs – estimated at an average of more than $2m per company. This is above the typical costs in other sectors, and Sophos attributes this fact to the highly regulated nature of the industry. One odd feature is that only 8% of organisations were hit with 'double extortion' attacks, in which a compromised target has data stolen and, after paying to decrypt its files, is blackmailed again with the threat of the data being leaked. There's more information here: https://bit.ly/3lnICoM.

New home for USAF cyber wing

The town of Mansfield, Ohio – which earned the nickname 'Danger City' in the 1970s – is to be the new home of the US Air Force's Cyber Warfare Wing. The 179th Airlift Wing currently based at the Mansfield-Lahm Air National Guard Base will retire its eight C-130H Hercules aircraft and move over to the new, ground-based role. It's expected that an additional 175 military and civilian staff will be moved to the base. "I am extremely confident our airmen are capable of shifting focus from tactical air-land and airdrop operations to the cyber battlefield," said Col Todd Thomas, commander of the 179th.

Meanwhile, Gen Paul Nakasone, Commander, US Cyber Command and director of the National Security Agency, has told the Associated Press that he intends to create a 'surge' in cyber activities. "Even six months ago, we probably would have said, 'Ransomware, that's criminal activity'," Nakasone said. "But if it has an impact on a nation, like we've seen, then it becomes a national security issue. If it's a national security issue, then certainly we're going to surge toward it."

OpenSSL 3.0 released

After three years of development, version 3.0 of OpenSSL has finally been released. The open-source project saw more than 7,500 commits from over 350 individuals, and there were 17 alpha releases and two beta releases before the final version was ready. The Open SSL Project has warned that version 3.0 is not fully backwards compatible with the current version 1.1.1. "Most applications that worked with OpenSSL 1.1.1 will still work unchanged and will simply need to be recompiled (although you may see numerous compilation warnings about using deprecated APIs)," it said. "Some applications may need to make changes to compile and work correctly, and many applications will need to be changed to avoid the deprecations warnings." The changelog is here: https://bit.ly/3hvszDV.

Vulnerable databases

As the result of a five-year study, scanning 27,000 on-premise databases, Imperva has concluded that nearly half of them have at least one vulnerability that could leave them open to attack. On average, the databases had no fewer than 26 flaws with 56% of those being rated as high or critical severity. "Not only are businesses not investing enough effort into patching, but it seems some databases have just gone unnoticed as we identified CVEs dating back three and four years," said Elad Erez, chief innovation officer at Imperva. "For non-publicly accessible databases, attackers can use a range of tools such as SQL injections (SQLi) to exploit vulnerabilities in web applications that are connected to a database." There's more information here: https://bit.ly/3Ark1FX.

Threat Intelligence

HTML smuggling: analysing the ISOMorph attack

Tom McVey, Menlo Security

One of the leading cyber security concerns today is the exponentially expanding number of techniques that cyber criminals are rapidly adding to their arsenal.

Indeed, this year's statistics are already alarming. Cybersecurity Ventures predicts that cybercrime will inflict approximately $6tr worth of damage in 2021 – a figure greater than the economic output of all nations, barring the US and China (https://bit.ly/3BrrxAG). And come 2025, total costs are expected to rise further to $10.5tr, rising 15% a year for the next four years.

From data breaches and malware to ransomware, phishing and DDoS attacks, cybercrime continues to become more sophisticated and malicious by the day. Here, we'll be looking at the re-emergence of HTML smuggling, used by Nobelium, the group behind the SolarWinds and USAID attacks that came to light earlier this year.

Another recent example of an HTML smuggling attack is ISOMorph, which we recently identified. ISOMorph works using HTML smuggling, with the goal of delivering malicious files to its targeted endpoints. This is achieved through the evasion of network security solutions like sandboxes and legacy proxies.

Discord, a popular voice, video and text digital communication platform, has become the commonly used vector for such attacks. The Discord app is widely used, with over 150 million active users. Here, threat actors have been deploying remote access trojans (RATs) that have been specifically built to bypass and even disable commonly used defence methods, such as detection tools and anti-virus programs, before setting about logging passwords and exfiltrating data.

ISOMorph and the re-emergence of HTML smuggling isn't a huge surprise. Much like several other attack techniques and shifts in the cyber security environment that have occurred during the past 18 months, this has stemmed from the many changes brought about by the Covid-19 pandemic and the resultant 'new normal'.

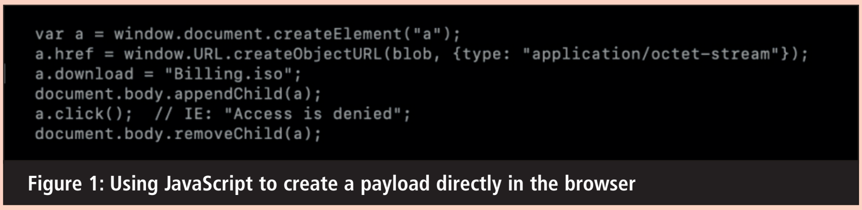
Where remote and hybrid working has become the norm, cloud-based models have risen to the fore, making the browser vital to day-to-day operations – from workflow management tools to virtual meetings.

Unfortunately, however, the browser remains as one of the weakest cyber security links and, as a result, attackers are able to use HTML smuggling to bypass network security solutions – including sandboxes, legacy proxies and firewalls – and deploy their payloads on victims' endpoints.

To explain how ISOMorph works in greater detail, it is worth considering an example of what an attack might look like. In our analysis, we have seen attackers leveraging HTML smuggling using both email attachments and web drive-by downloads. Using JavaScript, attackers construct a malicious payload on the HTML page rather than making a HTTP request to retrieve a desired asset from a web server (a technique often used by web developers to optimise file downloads).

In the case of ISOMorph, the JavaScript code was used to create a payload directly on the browser. In the example in Figure 1, the JavaScript code is creating an element ("a"), before setting the HREF to the blob and programmatically clicking it to trigger the download to the endpoint.

Once the payload is downloaded to the endpoint, the user must open it to execute the malicious code. With ISOMorph, the payload was an ISO file – a disk image that contains all the components needed to install software on endpoints that do not require any third-party software to install.



```
var a = window.document.createElement("a");
a.href = window.URL.createObjectURL(blob, {type: "application/octet-stream"});
a.download = "Billing.iso";
document.body.appendChild(a);
a.click();  // IE: "Access is denied";
document.body.removeChild(a);
```

Figure 1: Using JavaScript to create a payload directly in the browser

Many file formats are exempt from inspection across both web and email gateway devices. It is these file formats that are incorporated into their tactics, techniques and procedures (TTPs), with ISO files being one such example.

In our analysis of an ISO file, the VBScript will often contain many different malicious scripts capable of executing, before fetching additional PowerShell scripts that can download a file to the endpoint. ISOMorph also achieves persistence by creating a Windows directory.

> *"To truly combat novel attack styles such as these, it is vitally important that the initial access methods are identified and understood"*

In the campaigns that we have analysed, attackers execute the malicious code by proxy through tapping into MSBuild.exe – a trusted process that is typically whitelisted, allowing the injected code to go undetected. Reflection is also used to load a DLL file in memory and inject the RAT payload into MSBuild.exe, allowing attackers to bypass AV software.

A graph of the campaign that we've been tracking is publicly available on Virus Total (https://bit.ly/3mJ9DFn), where AsyncRAT is the remote access trojan that gets dropped to the endpoint.

HTML smuggling is likely to continue to grow in popularity – it is an effective method in which attackers can get their payloads to the endpoint while bypassing all network inspection and analysis tools. To truly combat novel attack styles such as these, it is vitally important that the initial access methods are identified and understood. This will help create a strong prevention, detection and response strategy.

And, as ever, for the ultimate endpoint detection strategy, isolation technology is highly effective.

Network security in the new world of work

Rodney Joffe

Rodney Joffe, Neustar

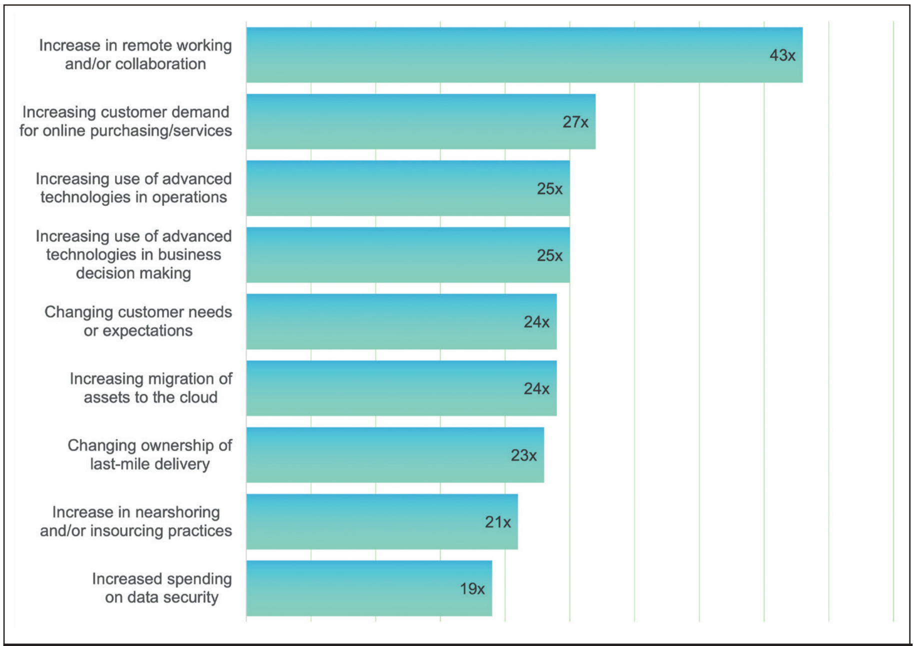
The largest networking security risks in the past year have been a direct result of organisations having to change the way they do business in an incredibly short space of time. According to a McKinsey study, in 2020 alone, digital offerings accelerated by approximately seven years.[1] While IT teams worked overtime to move nearly all operations online, cyber criminals monitored their every move, ready to exploit any issues stemming from the global disruption caused by new technology deployments and dispersed workforces.

As expected, businesses experienced a substantial amount of disturbance to their networks during the first six months of the pandemic. In fact, recent data revealed that 61% of cyber security professionals reported either significant or moderate downtime or disruption during this period due to the mass transition to remote working.[2]

Since then, the implementation of new collaboration and communication technologies, alongside improved cyber security awareness and protocols, have undeniably created a new set of security standards across all industries. Yet, despite organisations taking time to remedy the problems that initially came with deploying quick fixes, many challenges remain.

The research revealed that more than half (54%) of businesses have admitted to facing network security issues in the past six months, which is just 7% less than at the onset of the pandemic.

A large reason for this is that cyber criminals have become even more ruthless, stopping at nothing to capitalise on vulnerabilities within organisations' security postures – and in some cases this has had wide-reaching consequences. The situation came to a head in May when hackers gained access to Colonial Pipeline's computer system and shut off its oil flow – an incident that is being described as 'one of the most significant attacks to critical national infrastructure in history'.[3] However, while this particular case grabbed the headlines, attacks of all sizes are continuing to rise across the board. Last year, distributed denial of service (DDoS) attacks more than doubled when compared to 2019, with researchers seeing a sharp rise in ransom-related DDoS attacks (RDDoS).[4]



Wrought by the Covid-19 pandemic. The difference between the expected time to implement changes and the actual time, shown as an 'acceleration factor'. Source: McKinsey.

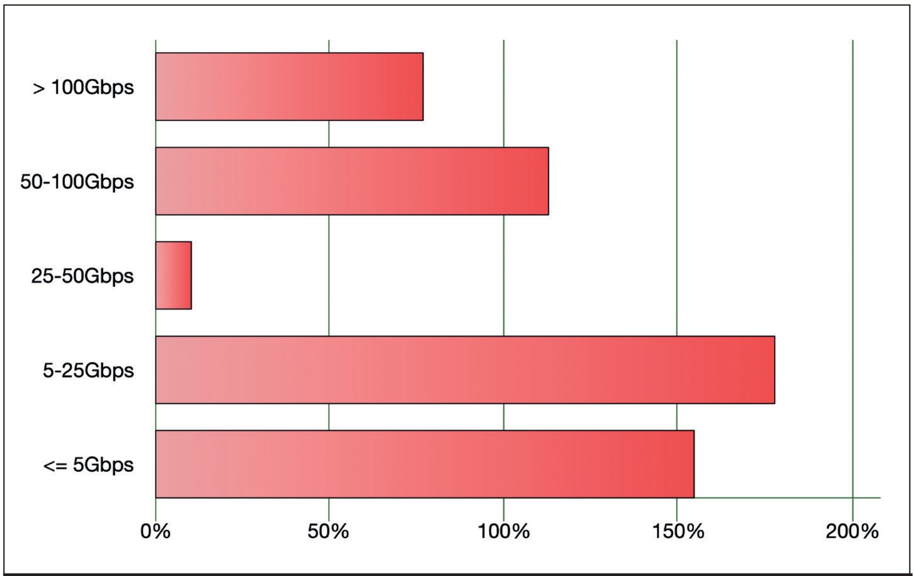
Amid all of the uncertainty of the past 18 months, it is clear that cyber criminals will continue to test the resiliency of our infrastructure well into the future. So how can security professionals reduce disruption and ensure that networks are secure as we move into the next era of work?

The VPN predicament

The majority of today's workplaces have had to transform irreversibly. A recent report revealed that 74% of employers now view workers' home-workspaces as an extension of their office, with 85% saying they expect to operate some form of hybrid working system moving forward.[5]

> *"Workers are linking a plethora of personal devices – such as computers, telephones and smart home devices – along with their work laptops. These appear publicly as a single IP address"*

In conjunction, corporate networks have also had to change to accommodate this shift. Whereas networking once happened in a supervised environment, it now takes place wherever employees choose to set up their remote working space. This means that, at any one time, a number of devices are connecting to a business' network – including home routers, cable or fibre modems and mifi devices. Behind these, workers are linking a plethora of personal



Percentage change in numbers of attacks between 2019 and 2020, per size category. Source: Neustar.

devices – such as computers, telephones and smart home devices – along with their work laptops. These appear publicly as a single IP address, so any infected device on the network can be used to infiltrate a system and cause a data breach.

In hybrid working environments, most of the tools and systems that employees interact with run in the cloud, which has specific security considerations. Core systems that store sensitive data, however, need to be operated locally and virtual private networks (VPNs) are key for giving employees remote access to systems.

While they are a business necessity, VPNs present a unique set of cyber security challenges to IT departments. Malicious actors are aware that the hardening of connectivity from a denial-of-service point of view hasn't always been done, especially during the pandemic rush. Following on from last year's supply chain attack on the SolarWinds Orion platform, the latest Cybersecurity and Infrastructure Security Agency (CISA) advisory said the agency recently responded to an advanced persistent threat (APT) actor's 'long-term compromise of an entity's enterprise network' that began in at least March 2020, the same month as the Covid-19 crisis.[6]

Because VPNs must be completely encrypted, teams cannot apply the usual techniques to inspect the traffic running through them. If a DDoS attack is contained within a VPN, organisations will only discover this when the packet is opened up as it reaches the VPN server. Unfortunately, at this point, teams cannot prevent the attack – only react to it.

Prioritising network security

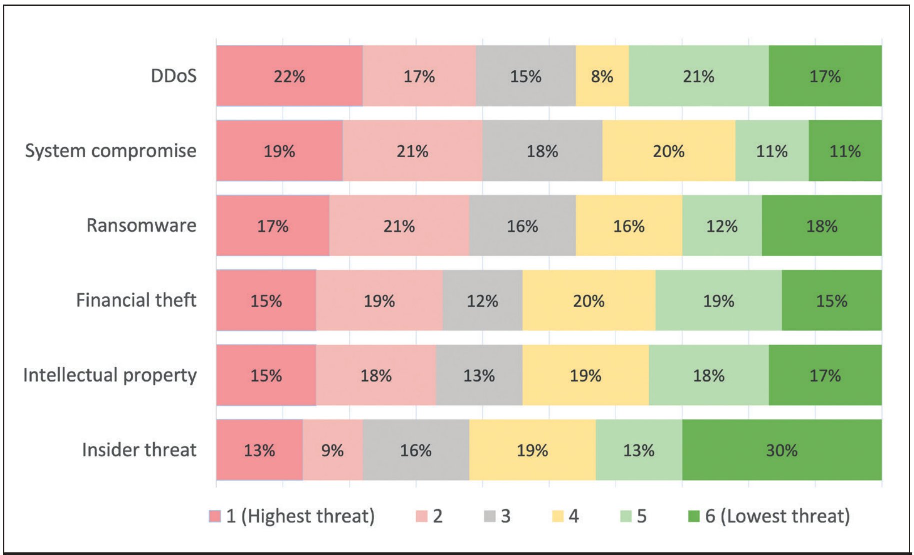
With hybrid working driving the need for stronger network security, organisations everywhere are navigating how to improve their defences – and work is already underway. Our research found that 79% of organisations have enhanced the security of their corporate VPNs over the last year. Not only that, 89% of security professionals have said that the challenges posed by the pandemic have boosted their organisation's network security against potential future attacks.

While progress is being made, though, businesses are still dealing with network disruption and downtime – and reducing this requires constantly reinforcing best practice security processes. Within distributed workforces, gaining a deeper understanding of what you have to protect is essential and making note of your business-critical assets is a key first step. This involves evaluating exactly where these assets are located and the threats they could fall victim to. Having an awareness of cyber threats that exist across different sectors is also key, particularly as attacks that were once contained to specific industries, such as RDDoS, are becoming more common.

Full picture

After getting this full picture, putting in place 24/7, always-on monitoring and mitigation should be top of the list. At this stage, it is important to remember that partnering with a third party can help provide holistic protection, especially if your in-house resources are stretched.

Your web applications should also be a main priority. According to new research, application-specific and web application attacks spiked last year, accounting for 67% of all attacks globally and more than doubling in the space of two years.[7] To help protect your infrastructure, you should ensure that your web application



Cyber threats ranked in order of concern from 1 (highest threat) to 6 (lowest threat). Source: Neustar.

firewall (WAF) defends against OWASP top vulnerabilities and enables virtual patching.[8] As part of protecting your application layer, you also need to bear in mind that cyber criminals are increasingly targeting the APIs of applications.

Everyone's business

Importantly, keeping networks safe in the new world of work is dependent on everyone in the business. Investing in education and training is crucial for getting cyber security right. Human error is consistently highlighted as one of the biggest threats to organisations, with research finding that 95% of data breaches are a result of an internal error.[9] All employees need to be aware of methods that are being frequently deployed to compromise devices, such as phishing and fake domains. Teaching the workforce how to identify these threats and take action is critical to an organisation's overall security stance.

The cyber security industry still has a long way to go when it comes to network security, but ultimately we are in a better position than we were before the pandemic. This year has demonstrated that adding more security and more resilience is not impossible – and now is the time for businesses to continue to push their security postures forward.

About the author

Rodney Joffe is SVP and fellow at Neustar, an information services and technology company. He is recognised across the industry as a global security pioneer and a serial entrepreneur. His computing career spans almost 50 years, long before the advent of personal computers. Besides being the founder of UltraDNS, which was acquired by Neustar in 2006, he was also the founder and creator of the very first Internet hosting company, Genuity, which was acquired by GTE in 1997.

References

1. 'How COVID-19 has pushed companies over the technology tipping point – and transformed business forever'. McKinsey & Company, 5 Oct 2020. Accessed Jul 2021. www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.
2. Neustar International Security Council survey. Neustar, 21 Apr 2021. Accessed Jul 2021. (Members only). www.nisc.neustar/nisc-survey-results/.
3. Tidy, Joe. 'Colonial hack: How did cyber-attackers shut off pipeline?'. BBC, 10 May 2021. Accessed Jul. 2021. www.bbc.co.uk/news/technology-57063636.
4. 'Cyber Threats & Trends: Securing your network pandemic-style'. Neustar. Jan 2021. Accessed Jul 2021. www.home.neustar/resources/whitepapers/cyber-threats-and-trends-pandemic-style.
5. 'TalkTalk Business Whitepaper: The impact of COVID-19 and levelling up hybrid working'. TalkTalk, Jun 2021. Accessed Jul 2021. www.talktalkbusiness.co.uk/partners/news-and-insight/white-papers/talktalk-business-whitepaper-the-impact-of-covid-19-and-levelling-up-hybrid-working/.
6. 'Analysis Report (AR21-112A): CISA identifies Supernova malware during incident response'. Cybersecurity & Infrastructure Security Agency (CISA), Apr 2021. Accessed Jul 2021. https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a.
7. '2021 Global Threat Intelligence Report'. NTT, May 2021. Accessed Jul 2021. https://hello.global.ntt/en-us/insights/2021-global-threat-intelligence-report/.
8. 'OWASP Top Ten'. OWASP, 2020. Accessed Jul 2021. https://owasp.org/www-project-top-ten/.
9. Milkovich, Devon. '15 alarming cyber security facts and stats'. Cybint Solutions, 23 Dec 2020. Accessed Jul 2021. www.cybintsolutions.com/cyber-security-facts-stats/

CPaaS and SASE: the best defences against IoT threats

Martin Giess

Martin Giess, EMnify

As the world goes digital and millions of devices connect to form the Internet of Things, IoT hacks are becoming a worrisome trend. These potentially devastating security breaches make strong IoT security an imperative for companies. Novel approaches like communications platform as a service (CPaaS) and secure access service edge (SASE) can help companies keep their connected devices secure.

The world is awash in smart devices. The number of devices that are connected to the Internet of things (IoT) is growing exponentially. According to Gartner, in 2020 there were 1.2 billion IoT devices communicating via cellular networks. The problem: the majority of the world's IoT devices are poorly secured. According to a 2020 study by Palo Alto Networks, 98% of all IoT traffic is currently unencrypted, and 57% of IoT devices have been subject to medium- or high-severity breaches. In sum, IoT devices face the inherent risk of being compromised by hackers and other malicious actors.

And as the industrial Internet of Things (IIot) grows exponentially, the frequency of security breaches of these devices and intrusions into smart device networks is also set to rise.

The threat is real

The Colonial Pipeline hack that happened in early May 2021 was a watershed moment as it underscored the vulnerability of critical physical infrastructure to security breaches. To be clear, it was the company's billing system (not the operational infrastructure) that was compromised. But the fact that hackers can so easily exploit a vulnerability and wreak havoc on millions of people's lives should give us pause.

The hack on the operator of the Colonial Pipeline was apparently carried out by a gang of cyber criminals who held the system to ransom. This attack caused enormous disruption across several US states and led to panic buying of petrol and diesel. Similarly, the recent attack on payment provider Visma Esscom, which exploited a vulnerability in the remote maintenance software VSA, by security company Kaseya, led to the closure of supermarkets like the Swedish CO-OP, impacting thousands of people.

> ***"Attacks on IoT devices will escalate, even as more smart devices are connected. The bottom line: IoT security should be a priority for every organisation"***

Any Internet-connected device can be targeted, hacked and exploited for nefarious purposes. Worse, as the IoT expands, more devices – many with inferior security standards – are being connected to it. This effectively lowers the technical bar for bad actors with malicious intent, and means that attacks on IoT devices will escalate, even as more smart devices are connected. The bottom line: IoT security should be a priority for every organisation.

To counter the evolving range of cyber security threats, experts need to evolve their security smarts in three ways:

1. Understand how and why their IoT applications and devices are vulnerable to hacking attempts.
2. Learn from past IoT security failures.
3. Apply solutions and strategies to harden the security of their applications.

Examining your network

One reason why IoT devices are so vulnerable to hacking attempts is the security – or lack thereof – of the network to which they are connected. Of course, using the public Internet to communicate is one (bad) thing, but this also applies to private networks with substandard security standards. Even if your network traffic is unencrypted, malicious actors can compromise IoT devices in myriad ways.

Eavesdropping and traffic sniffing: Poor encryption settings for data transmission make your communication vulnerable to hackers who want to read, steal or otherwise tamper with your data. This is an especially significant security threat for IoT networks as regular transmissions between and among devices are usually not encrypted. While encryption may not be needed for devices that do not store sensitive data, such as thermostats, an unsecured device and its unencrypted transmissions can still provide a hacker with an entry point into your wider network.

DNS poisoning: Another common threat stems from compromised public Domain Name System (DNS) servers. DNS poisoning is a tactic employed by malicious actors to divert and re-route communications between devices away from a legitimate application server to a spoofed one.

Distributed denial of service (DDoS): This is a well-documented approach by which a server is inundated with redundant requests, effectively overloading its capacity and often taking it completely offline. A DDoS is usually carried out from a botnet into which a large number of previously breached servers and computers have been subsumed.

Unprotected SIM: Many IoT devices are in publicly accessible locations (sensors on traffic lights, street lighting, ATMs and so on) where a bad actor can easily snatch them, breach them and steal the SIM card held inside the device and use it to tap into the company's data.

Calling home to base: Similarly, once malware has infected a device, it can re-program the device to 'call home' to the hacker's base, thereby sending sensitive data to malicious actors without the user's knowledge or consent.

Hackers are skilled at exploiting one of the weakest links in the security chain: humans. People – even seasoned security professionals – may opt for convenience over being bullet-proof. This may be intentional – they don't want the hassle of complex passwords and the need to frequently change them. This starkly drives home the point about 'password hygiene' and the need for effective policies that require human operators to use hard-to-crack passwords that are beyond the scope of a brute force attack.

Learning from the past

The old adage that 'the only constant is change' holds true for cyber security. Even though the technology used by hackers continues to evolve and new zero-day exploits are discovered on an almost daily basis, security professionals can still learn valuable lessons by analysing past security breaches and applying lessons learned to their network and security policies.

> ***"While encryption may not be needed for devices that do not store sensitive data, an unsecured device and its unencrypted transmissions can still provide a hacker with an entry point into your wider network"***

Part and parcel of this effort is understanding (or trying to understand) the motivations of malicious actors for intruding into your network. While the hack of the Colonial Pipeline was about extorting ransom payments, other attacks like the 2016 Mirai botnet case were solely about wreaking havoc. In 2016, a type of malware was being disseminated across the Internet. It eventually subsumed over 145,000 IP cameras into a botnet and then instigated DDoS attacks against the servers of the computer game Minecraft and the websites of companies such as Netflix, Twitter and Reddit.

Deficient topologies

Currently, a surprisingly large number of IoT network connectivity models rely on an approach that routes traffic first through the central LAN and then to the WAN (the public Internet) to the individual device's location. This comes with the territory, as some IoT networks extend across vast (often continental or global) distances, and so this is where cellular connections become important.

"Companies will need to deploy their connected devices over a cellular network wherever wifi is not a practical solution. This has been further complicated by the emergence of SaaS applications"

To keep communications secure, traditional networks make use of a complex setup of dedicated endpoint clients that are needed to establish a VPN connection or use SSL/TLS encryption between the various IoT endpoints and the application that processes their data. Unfortunately, this topography is no longer up to the task of securing communications due to the exploding number of new devices that are being added to the IoT, enabled by new connectivity models such as wifi and Zigbee and the overall miniaturisation and decreased cost of these devices.

What this means for companies is that they will need to deploy their connected devices over a cellular network wherever wifi is not a practical solution. This has been further complicated by the emergence of SaaS applications and the need to efficiently (and securely) transport large volumes of device traffic into the cloud.

Clearly, cellular IoT applications require a new approach to both network topology and security technology.

Dedicated IoT cloud

Enter CPaaS. The shortcomings of the prevalent approach have led to the design of a new model. To efficiently manage and process thousands of connected IoT devices, companies need a dedicated cloud that is optimised for the task. CPaaS offers unique advantages.

IT consulting firm Gartner defines the CPaaS model as offering "a cloud-based, multilayered middleware on which (companies) can develop, run and distribute communications software."[1] A CPaaS provides companies with application programming interfaces (APIs) so they can easily integrate communication channels into their applications. While the model was originally designed for a person-to-person context (such as voice or video messaging), CPaaS has evolved to cater to the various technical requirements of IoT applications.

With CPaaS providing the stack architecture for IoT applications, it became clear that a better approach for security was needed.

Adding SASE

SASE (pronounced 'sassy') was a term coined by Gartner in its '2019 Networking Hype Cycle and Market Trends' report. The term popularised a new cloud architecture concept in which the networking and security functions are bundled together and delivered as a single service via the cloud.

The SASE concept is characterised by a global cloud-native architecture, identity-driven services, central policy control and distributed security enforcement. Using SASE, organisations can integrate their network and security tools into a single management console. This gives them greater visibility of all their traffic and communications.

Originally developed to suit the changing requirements of an increasingly remote and globally distributed workforce that required access to enterprise IT infrastructure, SASE really came into its own as the best way to manage IoT devices.

In essence, multiple virtualised networking and security applications are converged through SASE into a single unified cloud service offering. A centralised policy control system helps to deliver secure access to clients by offering optimised data routing and the protection of communications traffic to the various individual applications. This is independent of where the device, network and IoT application are located.

SASE is optimised for IoT

The SASE model differs markedly from traditional networking models in several ways. First, it locates security checkpoints closer to the original data source. Next, the various policies (such as access protocols) are administered at distributed points of presence (PoP).

These PoPs can be a SASE vendor's datacentres or cloud regions, if located in relatively close proximity to the device in question. Access is granted upon verification of the identity of the IoT device. A device can be identified based on specific attributes or its location. Furthermore, the policies themselves are programmable and can be tailored to the needs of individual applications.

"A centralised policy control system helps to deliver secure access to clients by offering optimised data routing and the protection of communications traffic"

As SASE combines a cloud-based and centralised system for policy management, as well as the local enforcement of identity-driven services, this model gives users the best of both worlds. Utilising the cloud clarifies cost and complexity as all network security services can be consolidated using a single vendor, which allows users to have a comprehensive overview of all communications among managed devices.

By leveraging edge computing, network latency is minimised. This enables companies that depend on large numbers of IoT devices to comply with any local data-processing requirements their customers may have and ensures high-performance security for these devices.

Furthermore, SASE differs from a traditional model in other important areas.

Remote access to on-premise resources: Whereas traditional models depend largely on VPN technology and SSL encryption or make use of a dedicated endpoint client, SASE acts as a VPN replacement. As part of this, IoT devices connect to a SASE to access on-premise or cloud services and the relevant policies are defined and applied through the SASE API.

Access to cloud resources: In a traditional network setting, cellular access of IoT devices to cloud resources is treated like any other online asset, using traditional firewalls, proxies and normal access to the public Internet. A SASE, on the other hand, provides IoT devices with optimised, streamlined, cloud-aware network access.

Networks and Internet access: It is complicated to access a cellular network through a traditional software-defined wide area network (SD-WAN) enterprise architecture. A SASE service integrates cellular access and traffic optimisation capabilities into a cloud service. This greatly facilitates connectivity between devices.

Back-end application security: In the traditional model, firewalls, or web application firewalls (WAF) and back-end services are usually separate and distinct applications or platforms, which makes integration cumbersome. A SASE, however, provides policing and identity-based access control from a central location, giving users a comprehensive view of network topology and activity.

Network access control: Standalone IoT devices rely on local configuration settings and software components to control network activity. Instead, SASE services aggregate a number of network security and access control – including firewalls as a service – into one unified fabric.

Delivering features

A modern SASE architecture can deliver a whole gamut of different network and security features. However, these may vary across different vendors' offerings. Some examples that may be regarded as essential, however, include:

- **Dynamic data routing with SD-WAN:** Using SASE, network access and traffic optimisation are integrated in an infrastructure setup that is distributed across the globe and makes use of multi-regional PoPs. Having access control and security policy enforcement as a cloud-based service eliminates the need for users to divert communications traffic through a vendor's own network. Routing data instead to a SASE PoP located in proximity to the device greatly reduces the latency of the IoT application in question.
- **Firewall as a service (FaaS):** Using a cloud-based FaaS is an effective solution to filtering out unwanted and potentially malicious Internet traffic and thereby protecting services delivered on the edge.
- **Cloud access security broker (CASB):** A CASB secures transmissions into multiple cloud environments against eavesdropping, traffic sniffing and data theft by thoroughly encrypting them.
- **DNS security:** By enabling users to configure trusted DNS services, a SASE solution helps them to protect the integrity and availability of their DNS.
- **Threat detection:** Lastly, SASE services provide users with complete visibility of the network and drilled-down event metrics to help them do a root cause analysis on any anomalies that may have arisen in their IoT solution.

Getting started

Here's how to get started with CPaaS and SASE. First, undertake an audit of where your company stands regarding connected devices. What network topography do you use? Do you already make use of cellular connectivity for your IoT devices?

Next, see which of your devices are at the greatest risk, and assess what these risks are. Finally, perform a gap analysis to see how your current infrastructure compares with a CPaaS and SASE environment. If your findings show that a CPaaS and SASE environment is superior to your current model, you should consider upgrading to this better option.

Using the CPaaS deployment model and the SASE security architecture is an effective way to guard against the threats that confront IoT devices. A SASE enables users to effectively control all IoT data connections to the public Internet, an intranet, a SaaS cloud and their remote workforce.

As IoT adoption becomes widespread globally and IoT applications increasingly shift to the cloud, CPaaS and SASE will gain greater acceptance as businesses demand a combination of cloud-native security tools, local policy enforcement and enhanced visibility of their connected devices. Users benefit greatly from having their network and security functions in a single management console, which greatly increases their efficiency and economies of scale.

> ***"CPaaS and SASE will gain greater acceptance as businesses demand a combination of cloud-native security tools, local policy enforcement and enhanced visibility of their connected devices"***

The looming threat of security breaches and the increasing prevalence of actual intrusions into company networks make it imperative for IoT companies to always keep their defences up. A successful security breach could have devastating consequences for a company. The selection of state-of-the-art security technologies such as CPaaS and SASE can give businesses – and their customers – more assurance that they are protected.

About the author

As EMnify CTO and co-founder, Martin Giess oversees the technical execution of the company's product vision. He has 15 years of experience as a technology expert in agile development of innovative telecom services. Before founding EMnify, he held technical VP positions at Syniverse and MACH.

Reference

1. 'Communications Platform as a Service (CPaaS)'. Gartner. Accessed Sep 2021. www.gartner.com/en/information-technology/glossary/communications-platform-service-cpaas.

Turning breaches from losses to wins

Tamas Kadar

Tamas Kadar, SEON

It seems that every year, a new record is set for the number of records exposed in data breaches.[1] In 2020, that number was 37 billion individual records, jumping a staggering 141% from 2019. Major breaches included the theft of information from approximately 5.2 million guests of the Marriott hotel chain and 2.3 million data points from a Brazilian biometrics company.[2,3] Although the year is far from over, we can expect 2021 to be another record-breaking year, with the phone details of 533 million Facebook users already leaked.[4]

Although much is being done by companies and security experts to prevent data breaches, we are far from a time when we will see the total number of breaches start trending downwards. Until that happens, those of us working in the cyber security field need to find a way to make lemonade from the lemons we have been handed. Fortunately, there are multiple ways to use the information from data breaches to improve security, both on a personal and corporate level.

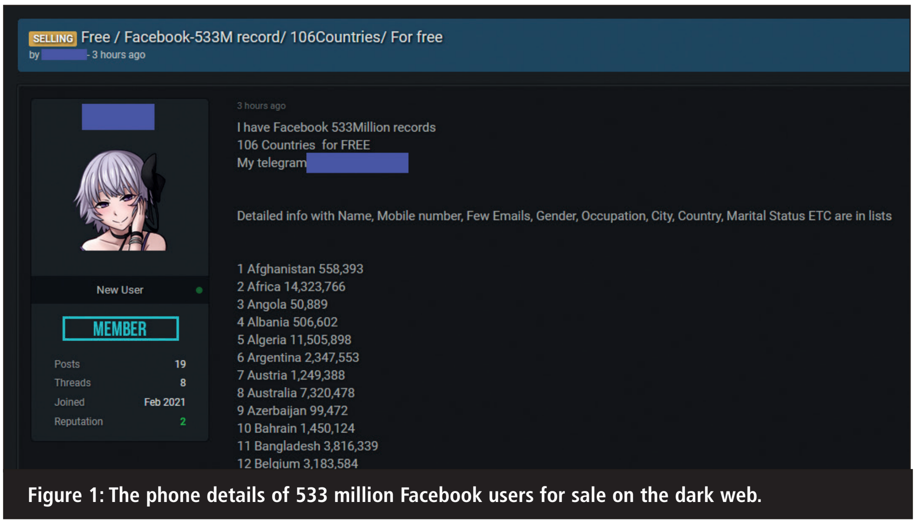
After a breach

Criminals rarely use the data they collect themselves – that would be a time-consuming process that would expose them to further risk. Instead, they package the data that they have collected and sell it on dark web forums.

In Figure 2, you can see that 21 million accounts from the music site Mixcloud were being sold for as little as $2,000 – and were available to as many buyers as were willing to pay. In this particular case, hackers would be unlikely to use the details on the Mixcloud site itself, since it has limited financial value. Instead, they would use the fact that between 31% and 55% of people use the same password on multiple sites to breach higher-value sites like Amazon or even banking sites, though both utilise more than an email and password for security.[5]

When an organisation becomes aware of a breach, it should email every affected user and ask them to change their passwords. Indeed, if the company is based in Europe, then General Data Protection Regulation (GDPR) rules mandate that they must contact all users. There is no way of knowing how many users will actually change their passwords, but it is unlikely to be 100%, so some information will still be usable to whoever purchased the data dump.

More importantly, even if all users change their passwords, few are likely to change the email address, which allows for fraud management professionals to increase the likelihood of determining which new sign-ups to a site are from legitimate and illegitimate users.



SELLING Free / Facebook-533M record/ 106Countries/ For free
by [redacted] - 3 hours ago

[redacted]

New User

MEMBER

Posts	19
Threads	8
Joined	Feb 2021
Reputation	2

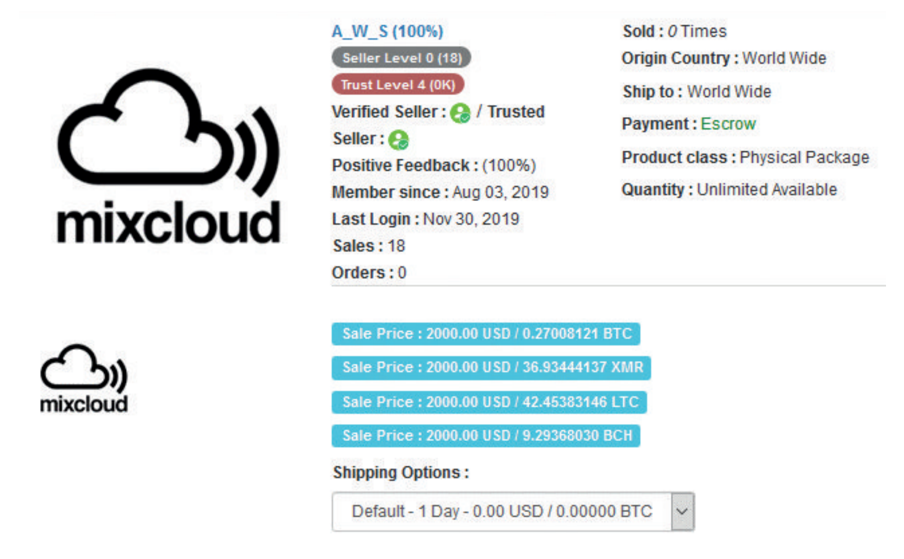
3 hours ago

I have Facebook 533Million records
106 Countries for FREE
My telegram [redacted]

Detailed info with Name, Mobile number, Few Emails, Gender, Occupation, City, Country, Marital Status ETC are in lists

1 Afghanistan 558,393
2 Africa 14,323,766
3 Angola 50,889
4 Albania 506,602
5 Algeria 11,505,898
6 Argentina 2,347,553
7 Austria 1,249,388
8 Australia 7,320,478
9 Azerbaijan 99,472
10 Bahrain 1,450,124
11 Bangladesh 3,816,339
12 Belgium 3,183,584

Figure 1: The phone details of 533 million Facebook users for sale on the dark web.



A_W_S (100%)
Seller Level 0 (18)
Trust Level 4 (0K)
Verified Seller : ✓ / Trusted
Seller : ✓
Positive Feedback : (100%)
Member since : Aug 03, 2019
Last Login : Nov 30, 2019
Sales : 18
Orders : 0

Sold : *0* Times
Origin Country : World Wide
Ship to : World Wide
Payment : Escrow
Product class : Physical Package
Quantity : Unlimited Available

Sale Price : 2000.00 USD / 0.27008121 BTC
Sale Price : 2000.00 USD / 36.93444137 XMR
Sale Price : 2000.00 USD / 42.45383146 LTC
Sale Price : 2000.00 USD / 9.29368030 BCH

Shipping Options :
Default - 1 Day - 0.00 USD / 0.00000 BTC

Figure 2: The 21 million stolen account records from the music service Mixcloud, as they appeared on a dark website.

Checking sign-ups

Most people would think that an email that has appeared in a data dump would be automatically classed as high risk if it were used to create a new account on a site. After all, the sign-up request could easily be from somebody who has taken over an account. The truth is more complicated.

Just as a person with no credit history would be considered riskier to lend to than somebody with a lengthy credit history, even if there were problems with it, an email address that can be linked to multiple sites, particularly social media sites with a lengthy history of posts and engagement, will be much more likely to be authentic than one that has no history.

This process is known as data enrichment – using a single data point such as an email or phone number to establish credibility and 'score' a new user based on how likely it is that they are a legitimate user. There are multiple aspects to this, including:

- **Validity:** through SMTP checks, the email server can be pinged to see if it exists.
- **Usage**: Checking if the domain comes from temporary email services. If it is, the risk score increases.
- **Domain quality**: Is it free? When was it created? Does it require SMS or other verification to open it? How about recent updates? Just a number of data points that can give great insights into an email address validity. For instance, Gmail is free, but requires verification, whereas Protonmail allows anyone to sign up.
- **Address quality:** Legitimate users do not enter a string of letters and numbers as their email address, but somebody creating large numbers of email addresses might. Using string analysis, we compare it to the username and get a good guess on whether the email contains real names and words.
- **Blacklisting:** It is easy to see if the email address belongs to someone who has been barred from another platform.
- **Social media presence:** An account that has a social media presence, particularly a long-term and active presence, is likely to be real – though sophisticated fraud outfits are getting better at creating fake personas for accounts they control. According to intelligence analytics for the lending industry, 76% of customers who defaulted on their loans had no social media presence, meaning that they were likely to be fake accounts.

Mature addresses

An email address that appears in one or more data breaches is likely to be real. Its presence elsewhere on the Internet means that it is, in data enrichment terms, a 'mature' address, and it may be possible to infer its age if it appeared in a large data dump from several years ago.

Although this may seem counter-intuitive, an email address that *does not* appear in any data dumps should be considered riskier, all other things being equal, since it may have been newly created. Fraudsters are likely to only use emails from recently released data dumps, so if it appears on a list from several years ago then you can have greater certainty that it is genuine.

Having this sort of data about new sign-ups is useful in any e-commerce environment that could be the target of fraud. But it is particularly useful in modern credit scoring, which uses far more than just credit history to make decisions on lending.

Checking log-ins

Of course, a legitimate user could sign up to a site only to later have his or her data breached – perhaps he uses the same password on multiple sites and when site X is breached, hackers are now able to access sites Y and Z, which may contain more information or allow for fraudulent orders or transactions. The only way to protect against this is for sites to be part of fraud-prevention networks that will automatically flag emails that are part of data breaches whether they are new sign-ups or existing users.

Of course, an e-commerce site could not and should not exclude every user whose account may be compromised – with data breaches being so extensive there would be serious impediments to almost anyone buying or selling online. Instead, there are intelligent, automated means to determine if a compromised account is genuine that do not introduce unnecessary friction into a user's experience.

For example, if an email has recently appeared in a data breach, then rules could be set up to look for suspicious activity like logging in from a new device or location or making large purchases or transfers. Device fingerprinting is particularly helpful in this regard since fraudsters are unlikely to be able to tell which device a compromised account uses.

Although it does introduce an element of friction, it's important to suggest to customers whose emails have been part of a recent data breach to change their passwords. Showing potential fraudsters that you are aware of them and are taking active efforts to combat intrusions might be enough to persuade some to leave your site alone.

> ***"An e-commerce site could not and should not exclude every user whose account may be compromised – with data breaches being so extensive there would be serious impediments to almost anyone buying or selling online"***

There will, of course, be more sophisticated rule set-ups depending on the nature of particular sites, such as flagging accounts that appear on data breaches then immediately change their password. This could mean that they are a security-conscious Internet user *or* a fraudster attempting to lock a legitimate user out of their account while they use it.

Every data point

As always, nuance is the key – no one data point is a firm yes or no for the presence of fraud, so each log-in and sign-up attempt has to be considered holistically and on an individual basis. This is not something that humans can do without seriously impacting customer experience, which is why so many firms are turning to AI-based systems to carry out near-instantaneous audits.

As we go into what is almost certainly another record-breaking year for data breaches, the security industry needs to use every tool at its disposal not just to prevent breaches but to use the information from breaches in their own security efforts. We can allow breaches to be losses or, by sharing information and best practices, we can turn them into wins.

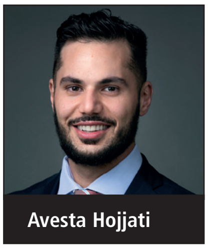
About the author

Tamas Kadar is the founder and CEO of SEON. He started the company with his co-founder when they were still at university and built it from scratch. A graduate of the Corvinus University, he studied deep info comms where he saw first-hand how fraudsters and hackers looked to get around security measures. He has been featured in Forbes' 'Hottest Young Start-ups in Europe' and is a regular start-up pitch winner.

References

1. Whitney, Lance. '2020 sees huge increase in records exposed in data breaches'. Techrepublic, 21 Jan 2021. Accessed May 2021. www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/.
2. 'Marriott International Notifies Guests of Property System Incident'. Marriot International, 31 Mar 2020. Accessed May 2021. https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident.
3. 'Brazil: Millions of Records Leaked, Including Biometric Data'. SafetyDetectives Cybersecurity Teamww, 11 Mar 2020. Accessed May 2021. www.safetydetectives.com/blog/antheus-leak-report/.
4. Cimpanu, Catalin. 'Phone numbers for 533 million Facebook users leaked on hacking forum'. The Record, 3 Apr 2021. Accessed May 2021. https://therecord.media/phone-numbers-for-533-million-facebook-users-leaked-on-hacking-forum/.
5. 'Reusing Passwords on Multiple Sites'. Centre for Internet Security. Accessed May 2021. www.cisecurity.org/blog/reusing-passwords-on-multiple-sites/#:~:text=Banking%20on%20the%20fact%20that,credentials%20at%20other%20popular%20sites.

The case for certificate automation



Avesta Hojjati

Avesta Hojjati, DigiCert

IT departments spend too much time on repetitive, manual tasks that eat up resources that could be spent on strategic initiatives.[1] And companies that are applying automation are realising benefits beyond just the time saved. Automation is transforming businesses and positioning them for competitive advantage.

Every business uses digital certificates and it's a great place to begin your automation. In this article, we'll look at six convincing reasons.

Short lifetimes

In September 2020, certificate lifetimes were shortened to a one-year maximum. This allows quicker updates to the certificate ecosystem, but it puts a strain on businesses and makes it cumbersome to manually manage your certificate inventory. Automation is no longer just a nice option. It's now essential in order to stay on top of certificate management.

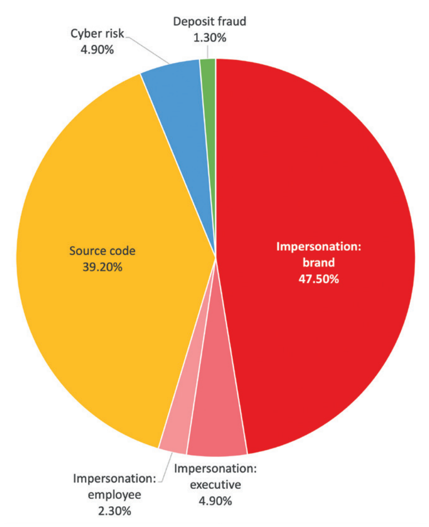
Shorter certificate lifetimes improve the security posture of your organisation – if you have the automation tools to discover and manage the certificate lifecycle. Automation also puts you ahead of the game when the inevitable requirements to upgrade to newer encryption algorithms arrive. And you can avoid the pain caused by past updates such as the transition from SHA-1 to SHA-2.

Sophisticated cyberthreats

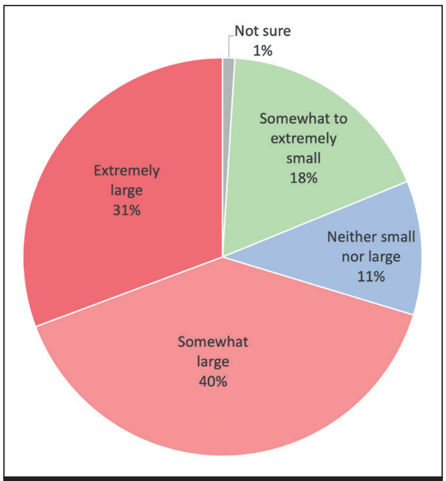
Security threats continue to get more sophisticated, making it increasingly difficult for IT to stay current on the latest threat. According to a recent report from PhishLabs, many threat actors use techniques such as impersonation, which are difficult to detect.[2] Automation processes make it easier for organisations to stay ahead of threats and respond quickly in case of breaches.

DigiCert's '2019 Post-Quantum Crypto Survey' found that 71% of IT professionals believe that quantum computing will present a major security threat in the near future.[3] Certificates that are not crypto-agile will leave networks susceptible to attacks.

We've been hearing about the vast potential of quantum computing for years. Last year we saw a lot of advances



Impersonation is common in the biggest social media threats to crypto-currencies. Source: PhishLabs.



Some 71% of organisations believe that quantum computing will represent either a 'somewhat' or 'extremely' large security threat in the future. Source: DigiCert.

and current innovation is pushing the technology closer to commercial adoption. We could see accessible quantum computing services in the next five or 10 years.

Now is the time to prepare. Organisations will need to move cryptography from using certificates with classic algorithms to post-quantum algorithms. Automation provides an efficient process for discovering outdated certificates that support pre-quantum cryptography and replacing them quickly.

Last year's transition to remote working has increased the threat risk and opened additional doors to hackers. They are leveraging additional vulnerabilities to breach corporate networks. In fact, Microsoft reported a large increase in attacks in March 2020 when the shift to remote work began.[4] Automation can help simplify remote management tasks to keep networks safe.

Efficiency

Automation increases productivity and performance as it frees IT staff to focus on strategic initiatives and other priorities. It also eases certification management and decreases human error. One survey found that over 40% of workers surveyed_spend a quarter of their work week on repetitive, manual tasks, and 60% estimate they could save at least six hours a week by implementing automation.[5]

With automation and discovery, IT can make quicker decisions with real-time, actionable insights into certificate inventory. This prevents revenue losses by giving IT the control and vision to make better decisions faster and remain compliant.

Many organisations have hundreds or thousands, or even millions of certificates to manage, making automation a vital requirement. Organisations that don't make the move will miss out on increased efficiency and lose their competitive advantage.

Certificate outages

The number of public key infrastructure (PKI) certificates that enterprises need to manage grew by 43% year-on-year in a recent Ponemon study , which means that the consequences of outages will also increase.[6] IBM's 'Cost of a Data Breach Report 2020' puts the cost at more than $500 per hour.[7] And it's not just the money. Repairing one expired certificate can take many hours or even days.

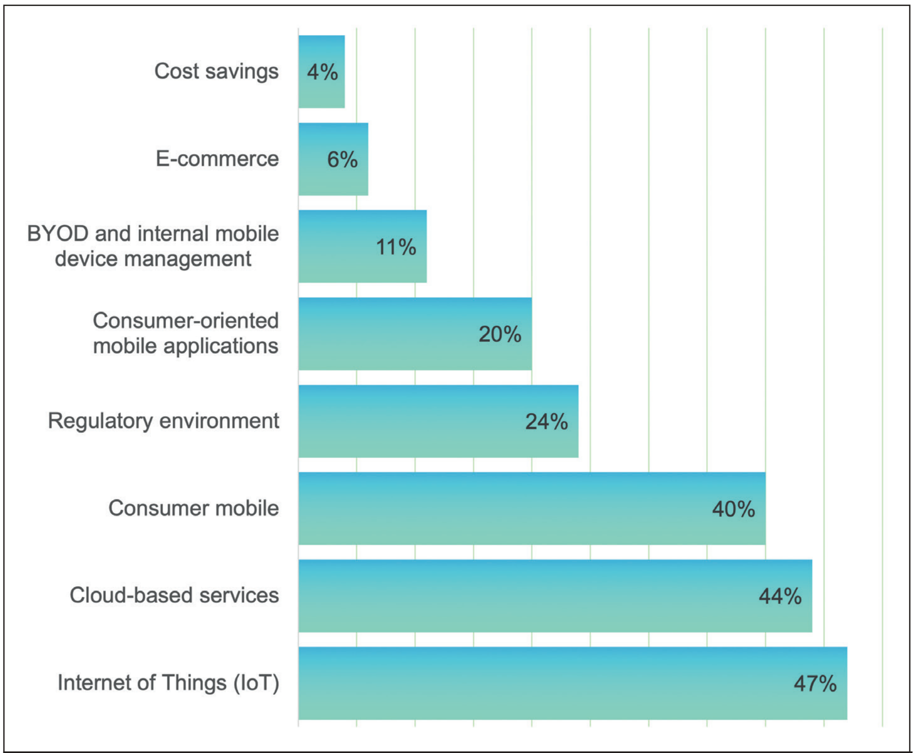
Companies also need to consider the damage to brand reputation and how that impacts customer relationships.

In April 2021, Fortnite experienced an issue with an expired certificate which caused an outage across a large portion of internal back-end service-to-service calls and internal management tools.[8] The outage caused issues for many of the company's games and services and prevented many gamers from playing Fortnite. Automation helps prevent downtimes and ensures that certificate renewal is fast and seamless.

Auditability and compliance

With the shortage of IT talent, and as resources continue to be at a premium, businesses may not have the personnel to assign a dedicated team member solely for certificate management, although it can be a full-time job. That's where automation can play an important role and enable organisations to keep up with industry changes and maintain certificate visibility.

However, many companies struggle and do not take the proper steps to ensure effective certificate management. The US National Security Agency (NSA), "emphatically recommends replacing obsolete protocol configurations with



The most important trends driving the deployment of applications using PKI. Source: Entrust/Ponemon Institute.

ones that utilise strong encryption and authentication to protect all sensitive information," such as TLS/SSL protocols.[9] It continues: "NSA recommends that only TLS 1.2 or TLS 1.3 be used, and that SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 not be used."

Obsolete and outdated encryption provides a false sense of security and leaves organisations at risk, providing resourced actors the ability to exploit weak communications using a variety of techniques, such as passive decryption and modification of traffic through man-in-the-middle attacks.

Automation also enables organisations to replace certificates quickly in case of an outage or a compliance issue that leads to revocation and replacement of certificates. These replacements for publicly trusted certificates typically need to be done within five days, according to CA/B Forum Baseline Requirements 4.9.1. This can decrease to as little as 24 hours for key compromise. In these instances, without automated revocation and renewal, certificate replacements in this short timeframe will cause only stress and problems down the road for the team.

About the author

Avesta Hojjati is the head of R&D at DigiCert, where he manages advanced development of cyber security products. Before joining DigiCert, he was part of the Symantec and Yahoo security teams, as well as operating his own cyber security startup. Hojjati focuses on applied cryptography, blockchain, post-quantum crypto and Internet of Things (IoT) security. He earned his master's degree in computer science with a concentration on security from the University of Illinois at Urbana Champaign, and he recently completed his PhD dissertation on applications of blockchain and IoT in manufacturing.

References

1. '7 Ways Manual Repetitive Tasks Are Eating Into Your Budget'. Impact, 29 Apr 2021. Accessed Aug 2021. www.impactmybiz.com/blog/blog-7_ways_repetitive_tasks_tech_budget/.
2. 'Quarterly Threat Trends & Intelligence Report'. PhishLabs. Accessed Aug 2021. https://info.phishlabs.com/quarterly-threat-trends-and-intelligence-august-2021.
3. 'Are you ready for the quantum leap?'. DigiCert. Accessed Aug 2021. www.digicert.com/tls-ssl/post-quantum-cryptography.
4. 'Microsoft report shows increasing sophistication of cyber threats'. Microsoft. Accessed Aug 2021. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/.
5. Beloof, Katy. 'How much time are you wasting on manual, repetitive tasks?'. SmartSheet. Accessed Aug 2021. www.smartsheet.com/content-center/product-news/automation/workers-waste-quarter-work-week-manual-repetitive-tasks.
6. '2020 Global PKI and IoT Trends Study'. Ponemon Institute. Accessed Aug 2021. www.ponemon.org/research/ponemon-library/security/2020-global-pki-and-iot-trends-study.html.
7. 'Cost of a Data Breach Report 2021'. IBM/Ponemon Institute. Accessed Aug 2021. www.ibm.com/security/data-breach.
8. 'April 6 – Technical Service Outage Report'. Epic Games, 16 Apr 2021. Accessed Aug 2021. www.epicgames.com/fortnite/en-US/news/april-6-technical-service-outage-report.
9. 'Eliminating obsolete Transport Layer Security (TLS) protocol configurations'. National Security Agency (NSA), Jan 2021. Accessed Aug 2021. https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF.

Reducing the security risks of USB devices

Rob Allen, Kingston Technology

Rob Allen

Data security is one of the biggest areas of risk faced by organisations and businesses of all sizes. But security is such a broad term and covers so many aspects of IT that it can be meaningless when referred to without additional context.

A list of the biggest and most obvious cyber security threats starts with the classic example of malware that may attempt to disable computer systems. But being secure also means protecting your networks from infiltration and data theft. It includes avoiding ransomware, where critical business data is locked until a hefty payment is made. It covers data loss from employees accidentally (or deliberately) mishandling company or user information, leading to it falling into the wrong hands. And it includes maintaining the security of employee credentials that can provide access to your data.

And that list only covers some of the more common security issues. Depending on the sector, more niche IT security problems may cause equal amounts of havoc for a firm.

Severe damage

These risks are a worry because of the severe potential damage they can do.

There are obvious financial risks. A severe breach means systems go offline, slowing day-to-day trade, and in the case of healthcare providers this could mean appointments are cancelled, which is what happened in 2017 when a number of NHS hospitals had to cancel appointments when systems were taken offline after a ransomware attack.[1]

In addition to lost business, there is the risk of legal fines from mishandling data. Despite Brexit, the UK equivalent of the General Data Protection Regulation (GDPR) is still law in the UK – meaning your business faces hefty fines for misusing customer data.

One of the most damaging potential consequences of a data breach is the theft of confidential company secrets. The loss of highly valuable R&D or intellectual property-related data, business plans and future product information that you're absolutely not ready to share with the public could affect every aspect of your organisation and future growth.

Similarly, you stand to lose customer trust after a data breach. It damages your brand and reputation, but if you botch the response – perhaps hiding crucial details about the data loss from customers, it could make the situation even worse.

Necessary steps

If a CISO explains these risks associated with data security to company decision-makers, the response is usually to take whatever steps are necessary to deal with them and avoid the potential consequences. Many of these measures are fairly straightforward and have now become mandatory IT security advice, as they are tried-and-tested ways to significantly reduce the likelihood of a business being damaged due to a data security incident.

This might include keeping all software and device firmware updated, installing anti-virus, anti-phishing and anti-ransomware tools, corporate VPNs, well-configured firewalls, physical security (including CCTV) and enforcing strong passwords. And in some companies, it includes enforcing the sole use of company-issued laptops, where centrally managed security policies are applied.

This lets managers sleep better at night, as they know the only way that employees are interacting with business data is on computers where said firewalls, anti-virus software, VPNs and perhaps even remote management software are mandatory.

The problem with USB

It may also mean disabling the USB ports on company computers, which can be a weakness in the defences of IT systems. USB devices may be shared among people, passed at trade shows and given away for free. Unwitting owners may use a USB stick with low-level malware on it that infects a host system or installs key loggers that would otherwise be detected by anti-malware tools.

"Losing a USB stick on a bus or train means that the spreadsheet is now in public circulation. An affordable USB stick may seem like a small loss, but it can do serious damage to a company if data is mishandled"

Additionally, there's a serious risk when using unencrypted USB sticks to regularly exchange data between locations – perhaps with databases or spreadsheets containing sensitive customer information or business plans. Losing a USB stick on a bus or train means that the spreadsheet is now in public circulation. An affordable USB stick may seem like a small loss, but it can do serious damage to a company if data is mishandled.

A quick and easy way to avoid these problems is to simply bring a very large IT security hammer down on them – by banning any USB devices in the workplace. But this can be complicated. Mitigating security risks involves bringing in measures that are often incongruous with today's trend of more-relaxed workplaces. Onsite gyms, free gourmet meals and even laundry services are offered as perks at some companies. And in the same way that few jobs now require employees in non-customer-facing roles to turn up for work in a suit, the trend is for companies to have rules in place that encourage the best possible productivity and flexibility – and this extends to corporate IT.

Personal devices

Many firms now have a bring-your-own-device (BYOD) approach to IT, allowing personal Macs, Windows PCs, tablets and phones to be used for work tasks, and these are integrated into company IT networks and access company data. This policy also often covers peripherals, such as personal cameras, microphones and printers.

In some cases, employees' personal computers are more up to date than corporate systems, with faster performance that allows better productivity; it's no surprise that many staff prefer to use their own devices. Likewise, disallowing the use of all USB peripherals may be an unnecessarily heavy-handed approach. The use of USB storage in the workplace offers many conveniences that help staff get their jobs done, making it easy to work from home and transport large amounts of data.

Pushing users away from USB just makes it more likely that they will use alternative insecure methods, such as sharing a company Excel database by sending it via a personal email account, or moving it onto Dropbox.

The solution

So how can firms continue to allow the use of USB without compromising security? The answer lies with encryption.

Any company can enforce software encryption using free tools built into Windows or indeed, other operating systems. This solution is far better than having no encryption at all, but there are some limitations to this approach.

By its nature it requires part of the encryption solution to reside on the host computer, hidden behind a password or key code. The computer itself, if lost or stolen, then becomes a weak point in the security of the data. If the password is captured via a key logger, it opens up access to the data as if the encryption was not there.

Additionally, software-based encryption requires CPU cycles to encrypt and decrypt data. As well as reducing read and write performance, it also reduces the performance of the host computer, as clock cycles are devoted to the decryption process.

Hardware-based encryption works differently. Encrypted USB drives are designed to protect the most sensitive data using the strictest security regulations and protocols. They have helped businesses large and small transport data when it needs to move beyond the company's firewall, securely and confidently. All encrypting and decrypting of data is performed on the drive itself, using internationally recognised secure AES 256-bit encryption standards.

"Encrypted USB drives are designed to protect the most sensitive data using the strictest security regulations and protocols. They have helped businesses large and small transport data when it needs to move beyond the company's firewall"

Hardware-encrypted USB drives are better protected against the possibility of brute-force, sniffing and memory hash attacks due to security being self-contained inside the drive. The drives allow a limited number of failed password attempts and if the number is exceeded, the data on the drive becomes totally inaccessible.

Beyond encryption

What's more, some vendors go to extra lengths to protect data on hardware-encrypted drives. Beyond just encryption, the design of the drive itself helps to prevent data loss from physical attacks, key logging and misplacing the device itself.

Physical access to the chips inside a device is one form of attack that cannot be wholly prevented, even though that data will remain encrypted even if the chips are accessed. However, security-conscious manufacturers seal USB drives with epoxy resin that cannot be broken without causing damage, making it evident that the drive has been tampered with.

Keyloggers can be foiled by avoiding password entry via the computer keyboard. Instead, access is restricted to passwords entered via an on-screen keyboard, with characters selected via the mouse or via an alphanumeric keypad embedded in the USB.

In corporate environments, serialised drives can help managers when devices are lost or stolen. When combined with managed access to company data, unique serial numbers and barcodes printed on the drive make it easier to know exactly who has each drive and therefore precisely which data might have been lost, making recovery a lot easier.

How does it work?

Self-encrypting drives use an on-board processor dedicated to AES encryption. This encrypts data before it is written to the NAND flash and decrypts it when data is read, without involving any resources from the host machine, or (in most cases) any encryption keys leaving the drive. With self-encrypting system drives that require a passphrase, this has to be entered on system boot via a custom BIOS, granting access to load the OS and data.

"The complexity of targeting keys in an SSD memory vastly reduces the likelihood of success. Aside from the use of a passphrase, this encryption is invisible to the user"

Since the keys reside in the memory of the drive itself rather than the host computer, many generic attacks designed to retrieve encryption keys are rendered useless. The complexity of targeting keys in an SSD memory vastly reduces the likelihood of success. Aside from the use of a passphrase, this encryption is invisible to the user.

The AES encryption algorithm used by the chip is symmetric, using the same key for both encryption and decryption of data. The data is divided into 128-bit blocks before encryption with a 256-bit key. For added peace of mind for a user who may not quite understand encryption, it may help to know that this level of security is an international standard, recognised by the US military and generally considered undecipherable and the strongest standard there is.

Why is it undecipherable? Every bit added to encryption keys doubles the possible number of decryption keys, so 256-bit encryption means 2^{256} possible keys – a number so big it would be impossible for any current computer to decrypt, or guess the correct key.

"Eliminating the host computer makes it much harder for a would-be attacker to extract data from a drive, and the off-system processing improves performance significantly"

The approach of hardware encryption, while fundamentally similar to software methods, makes data significantly more secure. Eliminating the host computer makes it much harder for a would-be attacker to extract data from a drive, and the off-system processing improves performance significantly.

About the author

Robert Allen is European director of marketing & technical services at Kingston Technology. He is responsible for the management of the technical services teams from customer services, technical support, RMA and Research and Development, as well as all the marketing and communications for the Kingston brand.

Reference

1. Griffin, Andrew. 'NHS hack: Cyber attack takes 16 hospitals offline as patients are turned away'. Independent, 12 May 2017. Accessed Sep 2021. www.independent.co.uk/news/uk/home-news/nhs-cyber attack-hack-hospitals-16-patients-turned-away-wanna-decryptor-a7733196.html.

The Firewall

Upgrading data privacy and protection

Fernando Guerrero Bautista, Airbus Cybersecurity

Information is the most important asset that companies have, only surpassed in value by people. Based on this premise, cyber security programmes should be focused on its protection, especially taking into account that attacks on data integrity and privacy are notorious crimes in recent times.

Digital transformation, including Industry 4.0, the new generation of cellular connection and the new interactions between companies, systems, networks and end users, form an ecosystem known as the data economy. These interactions often take place in collaborative environments, which allow an exchange of information among all of its members, often without restrictions.

In this context, the concept of data privacy involves the actions necessary for the collection, handling, processing and storage of information, according to a classification previously defined with its owner.

This concept becomes more palpable in the IT environment of those companies that, for one reason or another, obtain permission to handle personal information, including personal health information (PHI) or personally identifiable information (PII). This is especially true in the healthcare and financial sectors, government organisations, and basic public and social services. In this case, we are talking about medical records, bank accounts or transaction records, social security codes, dates of birth, names, and so on.

However, it is no less true that data privacy management is just as necessary in the operational technology (OT) environment. Companies that manage industrial control systems, or that are part of the critical infrastructure of a nation, also have data that forms part of the strategic information of the organisation and the operation or delivery of the service. Such information, if made public, could violate the privacy rights of workers. In industrial environments, we are talking about public and private IP addresses, user names, personnel names, records of operational actions, fingerprints and other biometric records, etc. In both cases (IT and OT), data privacy seeks to maintain the right of an individual (person or company) to have control over their own information and decide what happens to it.

This broad spectrum of data has led governments to generate different regulations with requirements that attempt to guarantee its protection. Currently, the best-known – including those oriented to specific industries – in the US are the GLBA, CCPA, HIPAA and FISMA: and in Europe, with application even beyond its geographical limits, the GDPR.

As part of the data handling, processing, collection and exchange processes, these regulations coincide with the need to include methods of suppression (removing sensitive information), generalisation (replacing sensitive information with more general but valuable information) and pseudo-anonymisation (replacing identifiable information with artificial identifiers), to the data protection strategy.

The recent wave of ransomware attacks (around 1,500 companies affected in the US alone in 2021 and 756 in Europe in 2020) has led data protection efforts to focus not only on maintaining appropriate regulation, but also on the development of new-generation technology – for example, with the use of machine learning – or the application of new security models, such as zero-trust.

Keeping the company's most important assets safe is everyone's responsibility and therefore, the most important point of any data protection strategy should be the generation of awareness in people through dedicated training and guidelines (such as the US Cybersecurity & Infrastructure Security Agency's for ransomware in OT).

Data privacy is a concept applicable both in organisations of all sizes and in people's daily lives, and finds its strength in data protection, which seeks to prevent misuse of non-public information. However, even though these concepts are known and regulated internationally, the need for their application is still latent.

EVENTS

Due to the Covid-19 pandemic, many conferences are being cancelled, postponed or converted into virtual events. The events listed here were still planned to proceed at the time of publication.

18–20 October 2021
(ISC)^2 Security Congress
Virtual event
https://congress.isc2.org

8–11 November 2021
Black Hat Europe
London, UK
www.blackhat.com/upcoming.html#europe

8–12 November 2021
OWASP Global Appsec USA
Virtual event
https://owasp.org/events/

14–15 November 2021
THOTCON
Chicago, IL, US
https://thotcon.org/

15–19 November 2021
Hack in Paris
Virtual event
https://hackinparis.com

16–18 November 2021
European Cyber Week
Rennes, France
https://en.european-cyber-week.eu

5–8 December 2021
Security Weekly Unlocked
Florida, US
https://events.securityweekly.com/unlocked2021

9–10 December 2021
ICCS
Cardiff, UK
https://iccs2021.iaasse.org/index.html

2–3 March 2022
Cloud & Cyber Security Expo
London, UK
www.cloudsecurityexpo.com