Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
security. Penetration testing – that long-established stalwart of challenging a company’s defences in a ‘white hat’ hacker way – can be used to show developers how their code was hacked and the damage that could have been done.

Also, auditing is about more than the technical aspects of security. Auditors will be interested to know how employees follow the policies. So, apart from providing the right training, it is important to communicate security policies across the development teams, and use version control – a standard in nearly every professional development environment – to help enforce security policies.

For instance, an auditor might want to compare documentation with established internal processes and these should match: otherwise, concerns will be raised. Version control systems can be used to ensure that all information comes from the same source and procedures.

Version control can also be used to control who has access to what within the development environment. Applying granular control and permissions can be aligned with security policies. For instance, people should be given what they need to carry out their jobs, but nothing more. This could prevent, as one example, a situation where access to code could in turn provide access to customer databases where information can be exfiltrated. This kind of control will help to reduce the number of developers either deliberately or inadvertently abusing data access, and narrow down the possible culprit.

Security starts with development
Visibility, culture, using the right tools and automating where it makes sense – these are all recurrent themes in ensuring that software development is better protected. Of course, securing any enterprise is an on-going, huge and ever-evolving battle, but it is definitely time to make sure that the creation of software is more secure, right from the very first steps.

About the author
With 25+ years industry experience, Rod Cope is chief technology officer within Perforce Software (www.perforce.com) and provides technical vision and architectural leadership for the company’s globally distributed teams. He was the founder and CTO of OpenLogic and joined Rogue Wave as CTO following the acquisition. For the past two decades, Cope has spoken on a wide variety of topics at events around the world. Apart from API management and security, other topics he has commented on recently include micro-services and multigrain services, agile methodologies, open banking standards, digital transformation and software development trends in general, especially at scale.

References
1. ‘OWASP TOP 10’. Open Web Application Security Project Foundation Accessed Jul 2020. https://owasp.org/www-project-top-ten/.
2. Bellairs, Richard. ‘What Are Secure Coding Standards: CERT and CWE’. Perforce Software, 8 Oct 2018. Accessed Jul 2020. www.perforce.com/blog/qac/secure-coding-standards.
3. ‘MISRA C and MISRA C++’. Perforce Software. Accessed Jul 2020. www.perforce.com/resources/qac/misra-c-cpp.
4. AUTOSAR, home page. Accessed Jul 2020. www.autosar.org.
5. ‘Common Weakness Enumeration’. Mitre. Accessed Jul 2020. https://cwe.mitre.org/.
6. ‘STRIDE (Security)’. Wikipedia. Accessed Jul 2020. https://en.wikipedia.org/wiki/STRIDE_(security).

The 2020 Data Breach Investigations Report – a CSO’s perspective
Martin Jartelius, Outpost24

There are few moments in the year where the cyber security industry will sit back and take note. One of those is the highly anticipated and much coveted ‘Data Breach Investigations Report’ (DBIR) by Verizon, which details the leading attack routes used by today’s hackers.1

Cyber criminals are ingenious beings, who will always look to pivot across systems until they find their end goal. Often this involves critical data being accessed by abusing weaknesses in the security infrastructure. The report is a deep dive that unearths common faults that are often symptomatic of data breaches, and highlights what actions need to be carried out in order to improve business cyber security.

To make the DBIR more digestible, there are four areas of concern that need to be flagged along with advice on how to effectively help the modern-day business to avoid suffering a similar fate to those detailed.

The phishing plague
When examining the DBIR, it was intriguing to read that 45% of security

---

**The 2020 Data Breach Investigations Report – a CSO’s perspective**

**Martin Jartelius, Outpost24**

There are few moments in the year where the cyber security industry will sit back and take note. One of those is the highly anticipated and much coveted ‘Data Breach Investigations Report’ (DBIR) by Verizon, which details the leading attack routes used by today’s hackers.¹

Cyber criminals are ingenious beings, who will always look to pivot across systems until they find their end goal. Often this involves critical data being accessed by abusing weaknesses in the security infrastructure. The report is a deep dive that unearths common faults that are often symptomatic of data breaches, and highlights what actions need to be carried out in order to improve business cyber security.

To make the DBIR more digestible, there are four areas of concern that need to be flagged along with advice on how to effectively help the modern-day business to avoid suffering a similar fate to those detailed.

**The phishing plague**

When examining the DBIR, it was intriguing to read that 45% of security
breaches took place as a result of hacking. Further investigation into these hacks revealed that 22% of these hacks occurred because the cyber criminal had targeted a member of the company’s workforce, with the preferred tactic being email phishing that most often included malware disguised as business documents. Phishing is widely known to be the most common of cyber threats and is highly successful because it plays on the naivety of humans.

Phishing attacks were also associated with an alarming rate of credential theft and social attacks (67%). Over a third (37%) of these credential theft breaches used stolen or weak credentials, of which 25% stemmed from a phishing attack, with human error being a contributing factor.

Throughout the coronavirus pandemic, cyber criminal activity has escalated as hackers try to take advantage of the situation and this has led to an increase in the number of social engineering attempts against businesses that are evidently struggling to adjust to managing the remote workforce. Given that most organisations have adopted a work-from-home approach, it is imperative to have a robust security awareness training programme for all staff members that includes regular sessions to build attentiveness to security threats particularly towards the tell-tale signs of phishing emails.

For additional support, organisations must ensure that their defences are adequate and must include blocking documents with active content, disallowing execution from the temporary email and browser folders, and keeping your users educated and security aware. While it may seem difficult under such conditions, security must not fall by the wayside.

**Application security issues grow**

Another interesting finding from the Verizon report is identifying where hackers are finding the most joy in terms of locating their initial footholds. According to the findings, 43% of breaches strike through web applications, with almost all (90%) of these attacks attributed to ‘hacking’.

Targeting the web application layer involves the already mentioned issues of weak, default or stolen credentials to actual technical exploitation of customer or standard vulnerabilities in the web application. With digital transformation sweeping most sectors, web application and cloud adoption rates are skyrocketing, and these are presenting more avenues for criminals to exploit. Yet, research has found that organisations are neglecting their security responsibilities in favour of rushing products to market as 31% of companies have admitted to prioritising speed over security standards.2

The DBIR report dives deeper into the issue of web application breaches and the data reveals that there has been a two-fold year-on-year increase in web application breaches to 43% overall. When looking at specific sectors, 81% of breaches within education and insurance have been attributed to web applications being exploited. Often information in such systems is stolen or encrypted in ransomware-like attacks. Negating this threat involves making the stolen information worthless by tokenising data and decreasing the risk of abuse of weak credentials by using multifactor authentication to add more layers of protection.

It’s clear the infrastructure around web applications is becoming a popular target for cyber attacks, and organisations must continuously monitor the security configurations within this area to prevent future attacks. This involves scanning applications against common vulnerabilities and testing for the recurring risks defined in frameworks such as OWASP Top 10.3

As more services and information transfers online, it can be difficult for businesses to keep track of where all the assets lie. It should be noted that while more or less any internal-facing application can benefit from automated scanning, one must also consider application logic and access controls, which also points to the need for penetration testing to identify critical vulnerabilities, particularly for mission-critical applications that process or store sensitive information.

**Mishaps in the cloud**

Given the numerous misconfigured cloud servers that have surfaced in the news of late, it is predictable to see that almost a quarter (24%) of breached systems involved cloud services. It seems to be almost weekly that poorly misconfigured cloud storage results in a breach of information regardless of whether it is AWS, Elasticsearch, Google Cloud, Dropbox or any of the multitude of additional third-party vendors, and it is severely costing businesses – $5tr in fact, according to a recent report.4 Yes, the cloud is a more efficient way to process or store data, but it certainly has its security challenges that must be addressed at deployment, which is the stage where there is a notable increase in the number of misconfigurations, especially if the implementation process was automated.
However, the most concerning aspect of cloud misconfigurations is that 80% were discovered by external observers – ie, outside security researchers, third parties or unsuspecting customers. Worryingly, if it’s this easy for outsiders, imagine how simple it is for hackers to exploit these services. Furthermore, it begs the question, why are these misconfigurations going undetected by basic security controls or security monitoring defences?

It is advisable for those investing in cloud services to conduct audits on the environments and the configurations set by the cloud provider. As a baseline, organisations can look to the CIS and CSA benchmarks to keep the cloud perimeter protected. Those wanting to take a more advanced strategy to securing multi-cloud environments should devote resources to automated cloud assessment tools, which can help alleviate the strain on security teams.

**Short time to exploit**

There may be some who think hackers will spend days or even weeks sitting behind a computer desk to infiltrate a system, trying to assault everything that comes in their path. However, this is often far from the truth as criminals usually do not execute advanced multi-step attacks. In reality, it takes hackers very few steps to steal the pot of gold (ie, data) or take down a system, irrespective of whether organisations have the necessary security in place. But why? Because the advantage will always be with the attacker and more so if the system is complex. Hackers thrive on businesses overcomplicating their security controls, because it allows them to navigate through the white space between the organisational siloes.

For example, avoid using accounts that have domain administration privileges when commissioning laptops, to prevent breaches of such credentials or permissions – this means that an incident targeting a laptop has less chance to, without further hacking, lead to the compromise of the domain and other key systems.

Also, it’s essential to take stock of what’s on the systems, which devices can access these systems, what applications are installed and taking the necessary precautionary measures to prevent untrusted devices from connecting to the network. If organisations batten down the hatches, hardening security configurations and centralising monitoring, inventory and vulnerability scanning, this will aid in finding any gaps in the security infrastructure and act as a necessary buffer.

**Prevention is key**

The Verizon DBIR 2020 report provides a fantastic insight into the current state of the cyber security world. It is evident that the number of threats is mounting and that hackers are constantly finding new means to cause devastation and disruption – some of which we’ve witnessed this year. Moreover, with the creation of international data security and
privacy regulations such as the General Data Protection Regulation (GDPR), organisations can no longer stay idle when it comes to acting on defending the network, given the serious repercussions of being found non-compliant when breached.

Remember, a hacker’s bread and butter is to feed off unpatched systems, and with digital transformation being widely adopted there is an increased likelihood that more of these flaws will become apparent. Therefore, security teams need to direct attention to mitigate risks within web applications, rogue access points and devices, and cloud environments that contain sensitive data.

Proactive identification of serious threats via automation and continuous scanning can be the difference between resolving a cheap risk or explaining a costly data breach. Yet technology can only do so much and there needs to be a focus on raising staff awareness and overall cyber hygiene. If all of these factors are addressed, then it will only be a matter of time before we see a decline in the number of easily avoidable, unnecessary breaches that make up the bulk of this year’s report. Once organisations start to realise that they need to get the basics of security right, the road to an effective and efficient strategy to avoid suffering a data breach will become much clearer.

About the author
Martin Jartelius is chief security officer at Outpost24. With a security-focused consulting background, he oversees every aspect of security at the company. His innovations initially introduced professional and managed services to the solution portfolio, and then established a strong security research team that has improved customer effectiveness in prioritising and remediating threats. As a former security consultant at Logical/CGI, Jartelius has specialised in security audits, compliance, IT forensics and penetration testing.

References
1. ‘Data Breach Investigations Report’. Verizon. Accessed Jul 2020. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
2. ‘RSA 2019 Survey’. Outpost24. Accessed Jul 2020. https://marketing.outpost24.com/mkg/whitepaper/rsa-it-security-survey-2019-outpost24.
3. ‘OWASP TOP 10’. Open Web Application Security Project Foundation Accessed Jul 2020. https://owasp.org/www-project-top-ten/.
4. Greig, Jonathan. ‘Cloud misconfigurations cost companies nearly $5 trillion’. Tech Republic, 20 Feb 2020. Accessed Jul 2020. www.techrepublic.com/article/cloud-misconfigurations-cost-companies-nearly-5-trillion/.

Avoiding the most common vulnerability-management pitfalls

Mieng Lim, Digital Defense

Vulnerability management (VM) can seem unmanageable at times. But the key to successful VM is working smarter rather than harder. If you approach VM intelligently and prioritise appropriately, you can keep the number of resulting tasks from spiralling out of control.

As with any ongoing security practice, there are countless ways you can botch VM. Often the devil is in the details as well as the larger processes. That’s why it’s good practice to step back and evaluate your vulnerability-management programme from end to end.

Below, we list a few common pitfalls that organisations need to avoid when it comes to vulnerability management.

Scanning slipups
It’s possible you are limiting your scanning to server-only or external-only scans. If so, you are missing the big picture. External scans look for vulnerabilities in your perimeter devices and defences that attackers could exploit.