Denial of Service attacks

1st Tobias Pilz
Web Security|Institute of Networks and Security
Johannes Kepler University
Linz, Austria
k11914471@students.jku.at

2nd Alexander Voglsperger
Web Security|Institute of Networks and Security
Johannes Kepler University
Linz, Austria
alexander.voglsperger@jku.at

***Abstract*—Denial-of-Service (DoS) attacks are one of the more common attacks that happen today. In this report, we want to talk about how they work and the various ways to implement them. Furthermore, we want to describe defensive measures to protect or at least mitigate them.**

***Index Terms*—Denial, Service, DoS, implementation, defense**

I. Introduction

We live in a very turbulent and fast-paced world. Since the year 2014 there are always continuing conflicts between Russia and Ukraine. Now, in the year 2022, these conflicts are escalating, territories are getting invaded, people fall in a war that has never been declared. In order to increase the own chances of a state in such a scenario, not only the infrastructure throughout the land has to be managed perfectly, but also networking is a factor that should not be let out. After the escalations started, one can see, that the count of cyberattacks is increasing rapidly. The most interesting part for this paper is, that the amount of DoS attacks in the first quarter of 2022 is about 46% higher than in Quarter 4 in 2021. But why is that? The answer is rather simple: In military conflicts, every part of supply-management is important, be it food, ammunition, or information. To prevent the enemy of distributing information, the easiest way would be to block all news-spreading websites, as people get their information mainly from the internet. In case of the Ukraine-conflicts, many official websites were being targeted by DoS attacks. But what are these attacks in detail? Are there different kinds of attacks? How do they work, and what can one do against them? All those questions are handled in this paper [1] [2].

II. Largest DoS event so far

On *June 1st* a customer of Google Cloud Armor (GCA) faced the largest HTTP-DDoS-Attack as of writing this paper. The attack peaked at around *46 million requests per second* and therefore is almost double the largest DoS-attack on *Cloudflare* before, with *26 million requests per second*. To make this number more tangible, 46 million request is what *Wikipedia* receives on a whole day. At the end, the lasted 69 minutes [3].

III. Types of Denial-of-Service attacks

A. Application-Layer-Attacks

Application-Layer-Attacks are sometimes also referred to *layer 7*-Attacks and try to exhaust server resources by sending Hypertext Transfer Protocol (HTTP)-requests. As an example, take a look at HTTP-flooding. A HTTP-request is lightweight to send, but may be resource intensive for the server to respond, this is an easy way to strain a server. The intensiveness for the server varies depending on if and from where resources are fetched. E. g. a database query requires more computational power than a simple read from a file. Therefore, when spamming a web-server with many requests, it is possible to slow it down or even crash it [4] [5].

B. Protocol-Attacks

The goal is to exhaust the server's resources by using flaws in the Network- and Transport-Layer's architecture. Attacks that fall under this category are as two examples the *SYN-Flooding*, which abuses the Transmission Control Protocol (TCP)'s three-way-handshake by sending many *SYN*-packages and occupying ports on the server to block legitimate

connections. The goal of Internet Control Message Protocol (ICMP) *Ping-Flooding* is to overload the Network Interface Card (NIC), by sending large amounts of *ping-requests*. This results in the NIC trying to keep up with answering these requests. *Smurf-Attacks* try to do almost the same as *ping-flooding*, but with the addition of broadcasting to the entire network and applying *origin-address-spoofing* to the requests. Such attacks are measured in Packets per Second (PPS) [6] [7].

C. Volumetric-Attacks

With *volumetric-attacks*, the goal is to clog the network connection by saturating the bandwidth the server has to offer. This congestion results in legitimate traffic not even reaching the server [8]. These attacks mostly consist of the above-mentioned *flooding attacks*. They are mainly achieved by using a *botnet* to execute so called Distributed DoS (DDoS)-attacks. It is not unheard of *volumetric-attacks* reaching *Giga-*, even *Terabits per second* and still rising [9] [10].

IV. Implementations

A. DDoS

When an attack does not only come from one, but from multiple machines, it is called a DDoS. As most attackers do not have the resources for such an attempt, DDoS attacks are mainly performed using compromised groups of devices, which are connected to the internet. They are controlled by the attacker, who uses software-handlers to hijack and control multiple devices. A general overview of the structure of this implementation can be seen in Fig. 1. The Botnets, as they are called, can also be rented to other attackers and can be used for several attacks through the internet. In case of DDoS, each bot sends requests to the victim, and as there are such many of them, this leads to an overload and therefore to DoS [4] [6] [11].

B. Application Layer

DDoS attacks usually target a specific weakness of the victim. As for application-layer DDoS attacks this would be the application-layer processes, or, referring to the OSI-Layer model, the seventh layer, giving them the name *layer 7 DDoS attacks*. One great example for this sort of attack is the

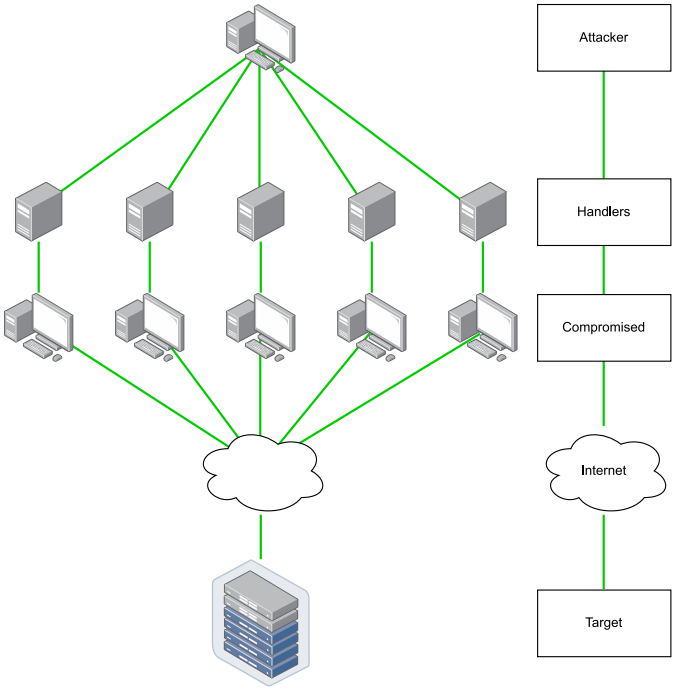

Fig. 1. Usual structure of DDoS attacks. Created by Tobias Pilz using https://draw.io

Slowloris DDoS attack. It sends HTTP requests that are not complete, which leads to the effect, that the server cannot yet process the request but keeps the connection open. *Slowloris* then opens more and more connections until the server cannot handle any more requests and all connections are waiting for the request to be completed. But *Slowloris* takes it even one step further and refreshes older connections once again by adding to the request, but not completing it. In other words, it simulates a very slow connection, but not that slow that the server closes the connection [12] [13].

C. Network layer

Another target layer is the networking-layer. As the *Network Layer* is the third layer in the *OSI-Model*, Network Layer DDoS is also referred to as *Layer 3 DDoS*. As the name already suggests, does this type attack the network equipment and the infrastructure of the victim. The main difference between other types of DDoS attacks and *Layer 3 DDoS* attacks is, that the attacker does not even establish a TCP connection to the victim. It suffices to send enough junk data to the target to slow down real connections and to finally block them. In more

severe cases, the networking components are heavily pressurized and may crash completely [14] [15]. According to *Cloudflare*, there are three major types of Network layer DDoS attacks:

- Ping flood: This form of DDoS attack uses only ICMP requests, one sends many echo requests to the server using multiple devices. As the server tries to respond to every request, he might run out of resources and the data flow starts slowing down until it even stop completely [16].
- Smurf attack: Another type of attack is the *Smurf attack*, which basically works like the *Ping flood*, but the attacker does not require lots of connections to other devices. The attack sends a ICMP package, with its source IP address altered to the victim's address, to a broadcasting address of a router which is connected to a big network. This router will then send the package to every device in the network, which will answer to the victim's IP as a consequence [17].
- Ping of Death: In this form of *Layer 3* attack, the attacker sends a ICMP ping request to the victim, but this time, the package exceeds the maximum size of such packages and therefore has to be fragmented by the routers on the way to the victim. When the victim tries to assemble and answer to the request, it crashes because of the package's size. [14].

D. Amplification attacks

The *Amplification attack* uses the behavior of a Domain Name System (DNS). The attacker alters the source IP again to the spoofed IP address of the victim. The DNS request the attacker is then going to send usually is for a domain with a lot DNS records. The more records there are, the more can the attack be amplified. When the attacker now uses only a few devices to send the previously prepared requests to multiple DNS servers, they will look up the domain and then send the result to the victim, normally overwhelming it by the amount of packages received. As *Amplification* is not really hard to achieve but can give the attack enormous power, it can be seen in many other *Network Layer* DoS attacks (IV-C) [18] [19].

E. DoS as a service (DoSaaS)

As you normally need to have the resources for a DoS attack, making business with just this kind of product has turned out to be quite lucrative. When some services to carry out such DoS attacks are offered to others, this is called DoSaaS. The services are usually based on the needed infrastructure, in this case mostly botnets. They are low-cost-high-effect tools, that act as a central reason for hundreds of attacks every year [20].

F. Permanent DoS (PDoS)

In most cases of DoS attacks, the victim can rather fast recover after the attacker stops the attack. But occasionally the effects of the incident are too dramatic, and the victims may not recover from them and is forced to replace their hardware, this is then called PDoS. The attacker attempts to sabotage the victim's hardware by exploiting certain firmware vulnerabilities. Most of the affected devices typically were not patched to the last update, and therefore it was possible to corrupt them. Usually PDoS attacks are more costly for the victim due to the fact that they have to replace their hardware, furthermore this attack type is cheaper for the attacker, since one does not need to rent a botnet for a certain time slot like in DDoS [21] [22] [23] [24].

G. Unintentional DoS (UDoS)

As we experienced in the last semesters when registering for courses through the Kepler University Study Support System (KUSSS) are unavailable websites. When analyzing these events, we can now conclude, that they are unintentionally executed DDoS attacks on the system of our university. The same implies for crashed services in *Moodle*, when more than 300 students try to submit online exams. Due to increased amounts of online exams because of the *Covid-19 pandemic*, our university started to use random offsets for every student to start the exam.

H. Side effects

DoS attacks do not only make the content not available for a certain amount of time, but also have other side effects one does not see at the first blink. On the one hand, an effect can be a damaged reputation: users, that normally rely on the service

may be upset and look for another service, that looks more resistant. On the other hand, if the attack was blocked, it can generate new customers. Another side effect is data loss due to corruption and rolling back to a previous version. The most important side effect are still the time and resources that have to be invested to recover from a DoS attack [25].

V. Defense measures

A. Reduction of a single Attack Area using Content Delivery Networks (CDN)

A CDN is due to its architecture, a globally spanned network of servers. They are designed to serve data to the end-user as fast as possible. They achieve this by caching versions of the original webpage and therefore reducing the load by only updating from the original server occasionally. Furthermore, the server's Internet Service Provider (ISP) can be configured in such a way that only traffic originating from a defined CDN is forwarded to the primary server. This makes it even harder to attack it, even when the IP-address got leaked. Such CDNs are designed to monitor, handle huge amounts of traffic and users around the world, they also apply automatic filtering to reduce potentially harmful traffic, as described in more detail in section (V-C) [26] [27].

B. Black holes and Sinkholes

A *blackhole* or sometimes also referred to a *sinkhole* describes the mechanism of a node to route network traffic into an equivalent of a real black hole. Such a network node can be configured to either block certain source-/destination-addresses or certain protocols. Traffic will go in but will be lost in there, and as with a real blackhole nothing will come out of out. Depending on the used protocol for the connection, the source won't even be able to detect a blackhole. This is due to only being detectable in lost traffic, or in case of TCP it will result in a ICMP response, of the node trying to forward, telling the source that the package could not be handed to the next node for transit. In general, Blackholing is pretty effective against harmful traffic, but also will route legitimate traffic into said blackhole. This might backfire, as this will definitely disrupt traffic, as the original attacker likely intended to accomplish with a DoS [28] [29]. But black holes can also backfire pretty bad. As an example, *Pakistan* banned *YouTube* with a blackhole. Due to an unfortunate event, this ban escaped through the Boarder Gateway Protocol (BGP) and effectively broadcasted to ISPs worldwide that they are the correct destination and then blackholed the world's traffic to YouTube [30].

C. Filtering Network Traffic

Filtering the bad traffic from the legitimate one is not that straight forward. There are many approaches to this, which come with different amount of wrongly discarded or permitted traffic. Filtering can also take place at different points in the network. The straight forward solution is filtering the of malicious traffic near the origin or at large internet backbones, where the traffic has to go through eventually. Mainly, the traffic is analyzed for patterns that are unusual for humans. Next to static filters, dynamic detection algorithms and machine learning is also applied for more effective filtering [31] [32].

D. Using a Firewall in combination with an Intrusion Prevention System (IPS)

A firewall has rules which try to block certain traffic. Those rules are often configured once and afterwards updated occasionally. An IPS is a piece of hard- or software which monitors a system or network for intruders. We mainly differentiate between the *Network-Based IPS (NIPS)* and *Host-Based IPS (HIPS)*. A NIPS analyses the network protocol traffic for potentially malicious traffic. On the other hand, HIPS runs on a system and analyzes connections, running programs and their log files. If any intrusion is detected, the system automatically deploys some kind of defense measure depending on the attack type. Such defense measures include removing harmful content, dropping packages, blocking an IP and notifying the system administrator [33] [34].

As a more practical example, *Fail2ban* is a HIPS and monitors the log files for enabled modules. Each module then applies filters on the corresponding log file. When an IP now shows malicious signs within a certain time threshold, *Fail2ban* adds the IP to a network filter or firewall, to stop further incoming packages. Depending on the configuration, the IP may get unblocked after a certain time. Most often,

Fail2ban is used for blocking brute-force attacks on SSH but can also prevent DoS and DDoS as it prevents IPs from accessing dynamically [35] [36].

E. Rate-Limitation and CAPTCHA

In general, *rate-limiting* describes the process of limiting requests. Mainly, this restriction is combined with a time period, but other versions like limiting on failed login attempts also exist. As an example, a website can set a limit to 20 request per 30 minutes. This can either be used for creating a subscription-based service or e. g. prevent login automated login. The second point here is the more interesting one, as it could also be a DoS or DDoS. Such limits can be based on different data-points, but normally are based on IP addresses or geolocation. It is possible to exempt users, e. g. when they are logged. Drawbacks with this solution is that automatic rate-limiting may also target real users in [37] [38] [39].

The Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a security measure to create tests for telling automated systems from humans apart. Those CAPTCHAs are often found at login/sign-up forms, comment section or e-commerce checkout pages. Such tests are designed to be easily solved by a human, but poses a challenge for bots and other automated systems. This type is also known as a *challenge-response authentication*. In the basic form, CAPTCHAs ask for typing down letters and numbers shown in a distorted image. In more advanced tests, the user has to pick images of certain objects. Those images often lack the proper resolution or are made from angles that algorithms have a hard time detecting them. A common implementation is the *reCAPTCHA* and was developed in 2009 by researchers at the *Carnegie Mellon University*, which then was later acquired by *Google*.There are a few drawbacks though. Captchas are not bulletproof and only can limit bad requests. They are also time-consuming and interrupt the flow of individual users [40] [41] [42].

F. DoS-attack response plans

To keep the service up and running, even if it being in a degraded state, it is important to have a response plan.

As a first step, make sure that you actually deal with an DoS attack and not just a surge in traffic. A upsurge in valid traffic often comes from a popular media report or a hype that references your service. It can also be helpful to report the incident to an appropriate government service or the police, when legal action is taken later on. Next, take a look at what kind of DoS attack it is and which part of your service is attacked specifically. The National Cyber Security Center (NCSC) recommends to not divert all security and network personal to the attack, as this may open other attack vectors. If not already done, deploying defense measures as described in (V) is essential. Also contact the ISP as they are often able to deploy measurements, before the attack reaches the service itself. At this point, informing the users about what is going on is a good idea. For this, use other forms of communication like email or existing social media accounts.

Oftentimes, dos-attacks come in bursts and often only last a few hours. But when an attack seems to have ended, keep defense measures up, as the attacker might just be waiting for them to get removed. And if you are sure that the attack stopped and the service recovered from it, make a review to see where things can be changed to make the service more resilient in the future [43] [44].

REFERENCES

[1] A. Gutnikov, O. Kupreev, and Y. Shmelev, "Kaspersky DDoS report, Q1 2022." https://securelist.com/ddos-attacks-in-q1-2022/106358/, Apr. 2022.

[2] BBC, "Ukraine cyber-attack: Russia to blame for hack, says Kyiv," *BBC News*, Jan. 2022.

[3] K. Emil and K. Satya, 08 2022.

[4] Cloudflare Inc., "What is a ddos attack?." https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. DDoS attacks are a primary concern in Internet security today. Explore details about how DDoS attacks function, and how they can be stopped.

[5] E. Chickowski, "Types of ddos attacks explained." https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained, 07 2020. AT&T Cybersecurity.

[6] Cybersecurity and Infrastructure Security Agency, "Understanding Denial-of-Service attacks." https://www.cisa.gov/uscert/ncas/tips/ST04-015, 09 2019.

[7] Bundesamt für Sicherheit in der Informationstechnik, "Dos- und ddos-attacken." https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html.

[8] IBM Cloud Internet Services, "Dealing with distributed denial of service attacks." https://cloud.ibm.com/docs/cis?topic=cis-distributed-denial-of-service-ddos-attack-concepts, 06 2019.

[9] Cloudflare Inc., "Famous ddos attacks — the largest ddos attacks of all time." https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/, 2021.

[10] T. Emmons, "Volumetric DDoS attacks rising fast." https://www.akamai.com/blog/security/2021-volumetric-ddos-attacks-rising-fast, 03 2021. Akamai Technologies.

[11] I. Belcic, "What is a botnet?." https://www.avast.com/c-botnet, 10 2021.

[12] Cloudflare Inc., "Slowloris ddos attack." https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/. The slowloris attack attempts to overwhelm a targeted server by opening and maintaining many simultaneous HTTP connections to the target.

[13] A. Sangodoyin, B. Modu, I. Awan, and J. Pagna Disso, "An approach to detecting distributed denial of service attacks in software defined networks," in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 436–443, 2018. doi=10.1109/FiCloud.2018.00069.

[14] Cloudflare Inc., "How do layer 3 ddos attacks work? — l3 ddos." https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/. Layer 3 DDoS attacks use layer 3 protocols, especially ICMP, to take down targeted servers, websites, or applications.

[15] D. Gargar, "Do Network Layer and Application Layer DDoS Attacks Differ?," Dec. 2021.

[16] Cloudflare Inc., "Ping (icmp) flood ddos attack." https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/. A ping flood is a type of DDoS attack that overwhelms a target with ICMP requests.

[17] Cloudflare Inc., "Smurf ddos attack." https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/. A smurf attack is a type of DDoS attack where a victim is flooded with ICMP requests.

[18] S. Teufel, T. A. Min, I. You, and E. Weippl, eds., *Availability, Reliability, and Security in Information Systems*, vol. 8708 of *Lecture Notes in Computer Science*. Cham: Springer International Publishing, 2014.

[19] R. Vaughn and G. Evron, "DNS Amplification Attacks," Mar. 2006. https://web.archive.org/web/20101214074629/http://www.isotf.org/news/DNS-Amplification-Attacks.pdf.

[20] B. Krebs, "Stress-Testing the Booter Services, Financially – Krebs on Security." https://krebsonsecurity.com/2015/08/stress-testing-the-booter-services-financially/, Aug. 2015.

[21] J. Leyden, "Phlashing attack thrashes embedded systems," May 2008.

[22] K. J. Higgins, "Permanent Denial-of-Service Attack Sabotages Hardware - Security/Management - DarkReading," May 2008.

[23] Radware, "'BrickerBot' Results In Permanent Denial-of-Service," Apr. 2017.

[24] EUSecWest, "EUSecWest Applied Security Conference: London, U.K.," Feb. 2009.

[25] Malwarebytes, "DDoS | What is a DDoS attack?."

[26] BelugaCDN, "Content Delivery Network Security - Increased Security Against DDoS Attacks with CDN Solutions." https://www.belugacdn.com/content-delivery-network-security/.

[27] Insight For Professionals and Inbox Insight Ltd, "Can a CDN Really Protect You Against DDoS Attacks." https://www.insightsforprofessionals.com/it/security/can-cdn-protect-you-against-ddos-attacks, 02 2021. A CDN is seen by some as a good way to guard against DDoS attacks. But how do these work, and do they really provide full protection?

[28] DE-CIX Management GmbH, "Blackholing service." https://www.de-cix.net/_Resources/Persistent/4/d/5/f/4d5f5d57cb3a466d34ea4d640961353f309ca6b3/DE-CIX%20Blackholing%20service.pdf. How to mitigate effects fo Distributed Denial of Service(DDoS) attacks.

[29] Cloudflare Inc., "What is blackhole routing?." https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/. Blackhole routing is a DDoS mitigation strategy that eliminates all traffic from certain sources.

[30] Iljitsch van Beijnum, "Insecure routing redirects youtube to pakistan." https://arstechnica.com/uncategorized/2008/02/insecure-routing-redirects-youtube-to-pakistan/. A black hole route to implement Pakistan's ban on YouTube got out into the ....

[31] K. Argyraki and D. Cheriton, "Active internet traffic filtering: Real-time response to denial of service attacks," 09 2003.

[32] W. J. Tann, J. T. J. Wei, J. Purba, and E. Chang, "Filtering ddos attacks from unlabeled network traffic data using online deep learning," *CoRR*, vol. abs/2012.06805, 2020.

[33] National Institute of Standards and Technology, "Guide to intrusion detection and prevention systems (idps)." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

[34] Barracuda Networks Inc., "Intrusion prevention system." https://www.barracuda.com/glossary/intrusion-prevention-system.

[35] Fail2ban, "Fail2ban main page." https://www.fail2ban.org/.

[36] Koen Van Impe, "What is a ddos attack?." https://securityintelligence.com/defending-against-apache-web-server-ddos-attacks/, 12 2015.

[37] T. Shostak, "Rate limiting: A vital part of modern web security," *Reblaze Technologies Ltd.*, 10 2020. https://www.reblaze.com/blog/cloud-security/rate-limiting-a-vital-part-of-modern-web-security/.

[38] Cloudflare Inc., "What is rate limiting?." https://www.cloudflare.com/learning/bots/what-is-rate-limiting/.

[39] Open Web Application Security Project, "Denial of serice cheatsheet." https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html#rate-limiting.

[40] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum, "reCAPTCHA: Human-Based Character Recognition via Web Security Measures," *Science*, vol. 321, no. 5895, pp. 1465–1468, 2008.

[41] K. T. Hanna and L. Rosencrance, "Captcha (completely automated public turing test to tell computers and humans apart)." https://www.techtarget.com/searchsecurity/definition/CAPTCHA, 11 2021.

[42] Cloudflare Inc., "What is a CAPTCHA?." https://www.cloudflare.com/learning/bots/how-captchas-work/.

[43] National Cyber Security Center, "Denial of service (dos) guidance." https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan, 1 2019. Guidance to help organisations understand and mitigate DoS attacks.

[44] CERT NZ, "Preparing for denial-of-service incidents." https://www.cert.govt.nz/it-specialists/guides/preparing-for-denial-of-service-incidents/. Denial-of-service (DoS) attacks aim to exhaust your resources and take your operations offline. They can have a significant effect on your business operations and are important to prepare for.