Threat Management in the Digital Business Age

Table of contents

White paper

Companies today are extending their traditional technology borders by leveraging cloud computing, social communication channels and mobile applications at various stages of business. Digitization has completely changed the way enterprises interact with their customers and partners. However, this also comes with a large number of threats and vulnerabilities that puts your sensitive customer data, intellectual property and business continuity at risk. Enterprise networks are becoming more complex and are in a constant state of change. This accelerated rate of change opens up new attack vectors and puts businesses in a constant state of compromise. Adding to the complexity, threat management is required by a growing number of regulatory bodies but it is challenging to stay compliant. When new risks are being introduced to your IT ecosystem every day, it is not only important to be up-to-date with the list of vulnerabilities but also effectively assess what threats are relevant to your business and how these threats can be mitigated. Software AG's Alfabet for enterprise architecture and IT planning and portfolio management provides an effective threat management solution to stay updated with product vulnerabilities, assess their relevance to your IT portfolio and perform risk assessment.

Threat management is the need of the hour

The IT ecosystem is vast with new application, infrastructure and operating system alerts being announced every day. The growing amount of security alerts indicates that security vulnerabilities exist in every organization. Dozens of security issues lurk in the IT environment which are neither discovered nor mitigated. The National Vulnerability Database (NVD), the U.S. government repository of standards-based vulnerability management data registers about 300-400 threat entries per week. This volume is overwhelming. The National Institute of Standards and Technology (NIST) reported over 16,000 official vulnerabilities in the first ten months of 2020 alone.

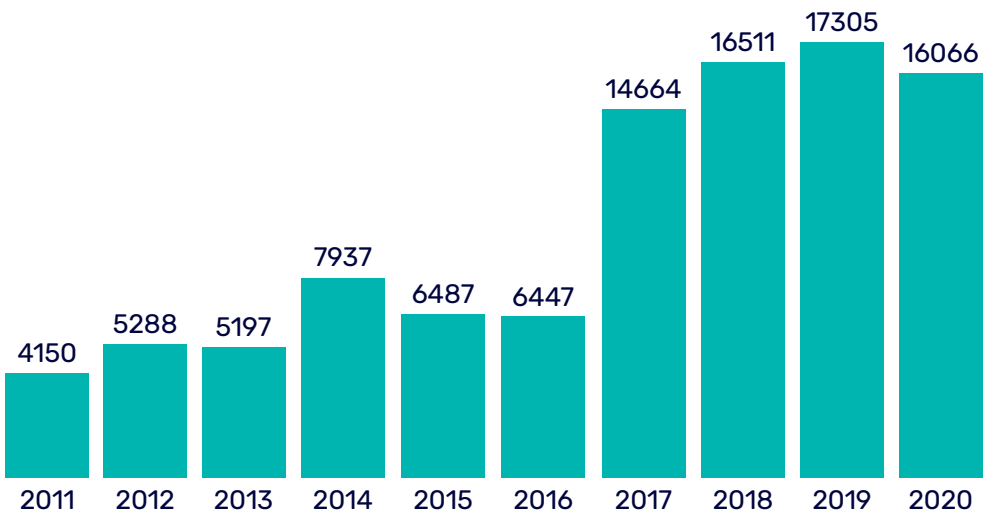

Figure 1: Reported Vulnerability by Year (Source: NIST, https://nvd.nist.gov/) .The table is updated as of October 2020.[1]

1 The jump in 2017 can be attributed to several factors—more software, more bug-bounty programs, new technology targets e.g. IoT, and improvements in assigning the Common Vulnerability Enumeration (CVE) identifiers. (Source: https://techbeacon.com/security/state-vulnerabilityreports-what-cve-surge-means)

Enterprise architects, portfolio managers and Security & Risk (S&R) professionals find it hard to stay up-to-date with the plethora of vulnerabilities and to address all of the security-related issues present within the IT ecosystem.

The Internet of Things (IoT) has ushered in a whole new dimension of threats. Gartner, Inc. forecasts that the enterprise and automotive Internet of Things (IoT) market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019 (https://www.gartner.com/en/news-room/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io). IoT security spending could reach $3.1 billion in 2021 (https://www.networkworld.com/article/3265075/iot-security-spending-to-spike-above-15-billion-in-the-next-year.html#nww-fsb). With the proliferation of the IoT, the number of vulnerabilities is increasing, thereby making your digital business vulnerable and prone to attacks. Enterprises are constantly trying to improve customer experience by culling the Internet and obtaining massive amounts of data points for analysis. Leveraging big data, cloud computing and encouraging a mobile workforce have become game changers for enterprises. However, with the rampant growth of digitization, enterprises are also under severe stress and risk due to vulnerabilities. Thus, threat management becomes increasingly important for enterprises to be able to take on these challenges confidently.

At an application level, security remains a crucial component to ensure that your data and enterprise servers are secure. Many firms have transformed their customer engagement process by developing mobile applications and building out websites to directly communicate with customers and partners without considering the security of the application itself. As a result, enterprises are exposing their most sensitive customer and corporate data to external threats and security breaches. In the Forrester report "Top Cybersecurity Threats In 2020", software vulnerabilities were the leading method for carrying out external attacks, and web applications were the second most popular avenue. Thus, enterprises need to put more emphasis on threat management and tackle software vulnerabilities.

Industry and government regulatory bodies have begun scrutinizing companies' risk management policies. Enterprises need to plan and manage strategies, architectures and processes with an understanding of all possible relevant threats and vulnerabilities in order to minimize risk. Staying compliant is extremely important for enterprises dealing with IT financial, healthcare and government institutions, as even a slight security breach can create a seriously adverse impact. Today, sophisticated hackers and cyber criminals target governments and corporations for valuable data that they can steal and easily monetize in the cyber underground, and also for more catastrophic reasons such as cyberwarfare, corporate shadowing, corporate sabotage and industrial sabotage. These adversaries are highly skilled, well-funded and, in some cases, state-sponsored, and their attacks are very sophisticated. Companies need to beef up their security and be under constant vigil to prevent any such attacks aimed at stealing sensitive information that could lead to grave consequences. Effective threat management is important to provide secure and compliant IT products and services to governments, healthcare institutions and commercial enterprises.

The impact of threats and vulnerabilities

Enterprise architects, portfolio managers and IT S&R professionals are often posed various questions concerning the security of the company's product and service offering and the IT that supports it. They are often called upon to help define the risk management practices of the organization. Some of the key threat management questions include:

- What are the relevant threats and vulnerabilities impacting the IT portfolio?
- How do we prioritize these threats?
- What should be the focus of the organization's threat management solution?
- How do these threats compare to our peers worldwide?
- What are the risks and challenges posed by certain vulnerabilities and how can they be addressed?
- How can we prevent future vulnerability exposure and mitigate the current threats?
- Do some of these risk concerns vary across industries?

Answering these questions can be a daunting task especially if there is no way to anticipate what could be coming down the line. Vulnerabilities can bear significant consequences both internally and externally. Here are a few of the impacts:

Non-compliance risk
A host of industry and government regulations mandate an active threat management program. Very often, we see enterprises making headlines and fighting cash heavy lawsuits for failing to meet with the federal guidelines. Failing to meet all state and federal compliance laws can result in serious consequences for a business. Along with altering a company's legal status, which may leave it vulnerable to lawsuits, government agencies may conduct audits, enact fines or even dissolve the business entirely.

Cybersecurity risk
In recent years, massive cyberattacks have resulted in extreme amounts of stolen intellectual property and personal data, leaving enterprises dumbfounded as to how it could have happened. Cybercriminals have become increasingly brash and are no longer only interested in ransom. Attacks resulting in data loss are usually performed by exploiting known and well-documented security vulnerabilities in software, network infrastructure, servers, workstations, phone systems, printers and employee devices. Online attacks on IT systems of public institutions and government organizations have debilitating effects and the aftermath is severe. Attackers are sharing information and developing new tools. According to the Verizon® Data Breach Investigations Report 2020, the highest amount of incidents among industries was in the professional, scientific and technical services sector (7,463 out of 32,002) followed by the public (6,843) and information sectors (5,471) sectors. This alarming rate of attacks on various industries indicates that no industry or organization is bulletproof when it comes to compromising data. On confirmation of data exfiltration, companies have to spend huge amounts to contain the damage. In the report "Cost of a Data Breach Report", IBM Security and Ponemon Institute determine the average total cost of a data breach at $3.92 million, with the highest industry average cost being $6.45 million in healthcare. And costs go on after the initial breach. The study reports 67% are in the first year, 22% in the second year after a breach and 11% come more than two years after a breach. Exposing your IT ecosystem to cybersecurity risk, thus, has cost and data loss implications.

Reputation damage
One of the major implications of not addressing security violations and vulnerabilities is damage to reputation. According to the AON® 2019 Global Risk Management Survey, compiled from responses from over 2,600 risk management professionals in 60 countries, reputation damage is one of the top ten risks, second only to economic slowdown/slow recovery. Reputation damage is closely tied to cybersecurity risk, basically arising due to ineffective threat management within an enterprise. When a data breach occurs, customer trust crumbles, revenues fall and shareholder value is badly diminished. Significant damage can result in plummeting stock prices. Sometimes, companies may have to engage in prolonged lawsuits. This not only hampers current customer relationships, but also acts as a major barrier for future business relationships. Customers become wary of the enterprise's threat management capability and may even pull out of business partnerships.

Unsound technology portfolio governance
Technology Portfolio Governance (TPG) aims at establishing a continuous process to monitor and evaluate technology trends and assess them with regard to their applicability to the enterprise. A TPG program's overarching goal is to deliver business value by establishing a catalog of technology standards that are used as fundamental building blocks for developing the enterprise's IT landscape. To establish these standards, develop the IT landscape and make key business decisions while laying out the IT strategy of the enterprise, it is important to have a complete overview of new and existing technologies including the threats associated with technology products. If threats are not assessed and managed, the enterprise IT environment is subject to risk. These threats and induced risks can interfere with demand management and project management activities, thereby preventing enterprises from delivering on business needs.

The reality is that your technology environment likely contains more vulnerabilities than your team can correct before the next batch rears its ugly head. Dealing with these threats and vulnerabilities is a formidable task. Even though plenty of threat management solutions are available, enterprise architects, portfolio managers and S&R professionals are met with a number of challenges to not only stay abreast with the newer vulnerabilities and threats, but also to tackle these effectively and mitigate them.

Threat management comes with a number of challenges

Although managing vulnerabilities is critical, organizations struggle to establish an effective threat management practice. Exploiting weaknesses in operating systems, networks, applications and other IT assets is often the first step in compromising a target. Forrester advocates getting a good understanding of asset criticality, vulnerability severity and network exposure to help prioritize remediation efforts. (The Forrester Wave™: Vulnerability Risk Management, Q4 2019). Despite the focus on vulnerabilities, it is hard for enterprises to address and mitigate them. Some of the main challenges involved in threat management are:

Keeping up with the growing number of vulnerabilities
Vulnerabilities come in different flavors targeting software, network controls, applications, Web applications, browsers, endpoints and more. Every day, new vulnerabilities are added to the IT ecosystem and enterprises are struggling to keep up-to-date with these new threats. Over hundreds of new threats are added per week. According to Verizon's 2020 Data Breach Investigations Report, it is worth it to keep adding patch after patch as "attackers will try easy-to-exploit vulnerabilities if they encounter them while driving around the Internet." As the saying goes: Opportunity makes a thief. Further, attackers are sharing information, automating certain weaponized vulnerabilities and spreading them across the Internet. The burgeoning rate of vulnerabilities is thus a major obstacle to enterprises implementing effective threat management solutions.

Lack of proper prioritization
Enterprises lack the time and resources to address this avalanche of threats and vulnerabilities. Remediating the most critical vulnerabilities is a constant challenge. To begin with, enterprises need to understand what threats are relevant to their IT landscape and how these threats can be prioritized. Not all threats can be addressed and mitigated on a regular basis. Thus, understanding the criticality and severity of these threats is important. Again, enterprises find it challenging to score these threats and prioritize them based on the severity of the impact they would cause to the IT landscape. S&R professionals are confused as whether to rely on vendor-supplied criticality measures, third-party metrics, such as CVSS, or develop their own set of metrics to assess these threats. Lack of proper prioritization of vulnerabilities is a great challenge in threat management.

Inefficient mitigation and remediation process
Once you identify that you are using technology that poses a threat, you can determine whether or not you have a risk and consequently need to determine how this risk should be mitigated or remediated. Security flaws are constantly addressed by the vendors who issue security patches and updates on an ongoing basis. In even modestly sized networks, making sure that all assets are running all the security patches can be a nightmare. A single host that is missing patches or that didn't get patches installed correctly can compromise the security of the network. All that patching is naught if you are not patching the right things.

Not every threat can be mitigated with a patch. Some might require an upgrade to a new version and that isn't necessarily easy. Some might not have a technology solution at all. So you might end up accepting certain risks associated with technology threats for an interim period, create plans to migrate off a certain technology that is exposing technology threats or take special precautionary measures to contain the risk, e.g., run the application in a separate domain or even a demilitarized zone, use only for internally facing applications or similar. Sometimes it is just not possible to fix a vulnerability—be it due to the lack of a patch, a business process impediment or incompatibilities. At that point, for whatever reason, you may have to live with those residual vulnerabilities. It's important to realize that mitigation is often just as useful as remediation—and sometimes it's your only option. But trying to understand how these vulnerabilities can be mitigated makes threat management difficult.

Alfabet's solution for threat management

Enterprises need to evaluate, plan and manage strategies, architectures and processes effectively by understanding possible vulnerabilities and threats. Threat management is required at every level of planning to reduce risk to your enterprise IT environment.

Software AG's Alfabet for enterprise architecture and IT planning and portfolio management provides an effective threat management solution to stay updated with product vulnerabilities, assess their relevance to your IT portfolio and perform risk assessment. The threat management process combines state-of-the-art vulnerability prioritization capabilities with risk assessment of vulnerabilities that help organizations identify the issues requiring immediate attention, so they can focus efforts on the vulnerabilities most likely to result in a breach.

The high-level process of threat management in Alfabet consists of four steps as illustrated in Figure 2.

Figure 2: High-Level Threat Management Process

The goal of the threat management process is to understand the most current and relevant IT vulnerabilities affecting the organization and effectively plan and monitor the actions needed to mitigate the impact of the risks posed by them. Data is imported from databases, such as the NVD. The NVD acts as a data source of the latest software products and their associated vulnerabilities. NVD, a product of the National Institute of Standards and Technology (NIST), is a database structured according to its products' unique Common Platform Enumeration (CPE) ID and their associated vulnerabilities that have a unique Common Vulnerabilities and Exposures (CVE) ID. A vulnerability can be associated with a number of products. Each vulnerability with a CVE ID is imported as a threat and classified into threat groups based on the product version. The latest threats can be easily uploaded from the NVD into Alfabet, thereby addressing the first challenge in threat management of keeping up-to-date with the growing number of vulnerabilities. Also, the newly imported threats and threat groups are categorized based on the learnings from the existing threat and threat groups, making this a continuously evolving system. The second challenge associated with threat management is assessing the relevance of the imported threats to the existing IT landscape. With Alfabet, you can start threat group assessment to assess the relevance of the threat groups to your existing IT portfolio.

Traditional threat management solutions scan vulnerabilities and assess their relevance to the existing technology landscape. However, they provide siloed results and prevent S&R professionals and enterprise architects from getting a clear overall picture of the risk involved. With Alfabet, it is possible to perform risk assessment and evaluation. The identified risks are evaluated for damage and likelihood of damage. This feature is effective in analyzing what vulnerabilities affect the IT and what the likely impacts are. With a greater understanding of what damage could be caused due to the applications exposed to threat, it is possible to develop a better strategy to prioritize and mitigate threats. Understanding the business impact provides a clear overall picture of the potential damage to the technology landscape and what this means to the enterprise.

The following screenshot from the Alfabet portfolio management product shows an information cockpit that revolves around the threat group “Microsoft®.” The top left chart displays the threat distribution over time and categorized according to the CVSS score of the threat severity. The chart next to it provides information on the threat distribution according to the CVSS severity score. CVSS (Common Vulnerability Scoring System) is an industry standard for assessing the severity of potential or actual security vulnerabilities in computer systems.. The Gantt chart on the bottom left shows the enterprise’s IT components that are associated with this threat group and life cycles. The chart on the bottom right displays the distribution of risks according to which ones will cause significant damage and the probability of it occuring (with and without mitigation measures).

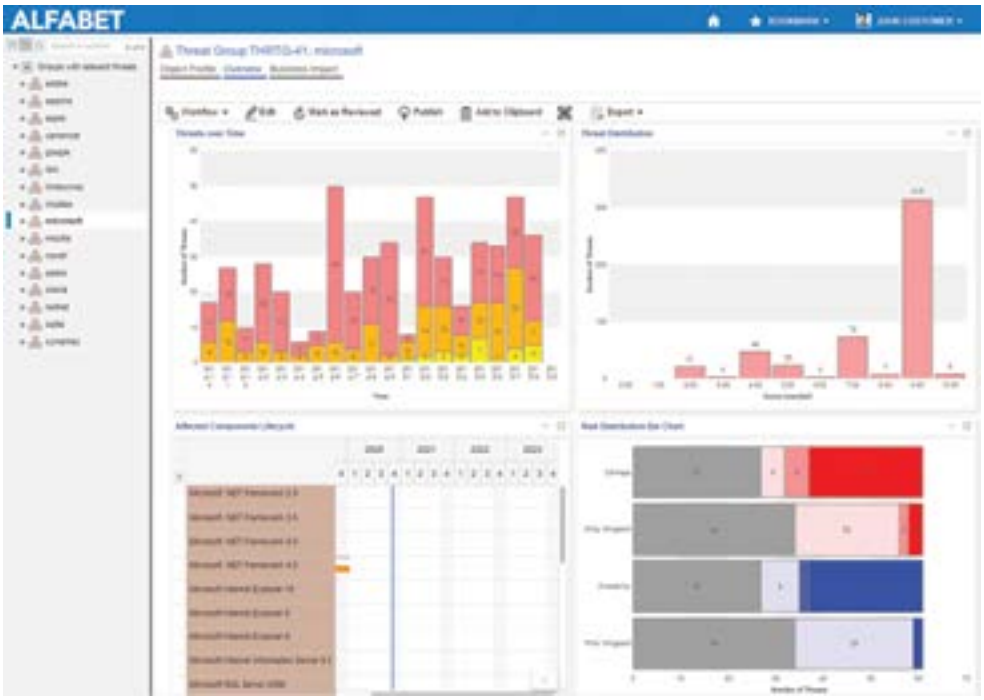

Figure 3: Threat Management Solution in Alfabet

The following business support map from Alfabet shows which processes (x-axis), organizations (y-axis) and applications (cells) are affected by the specified risk group “Microsoft.”

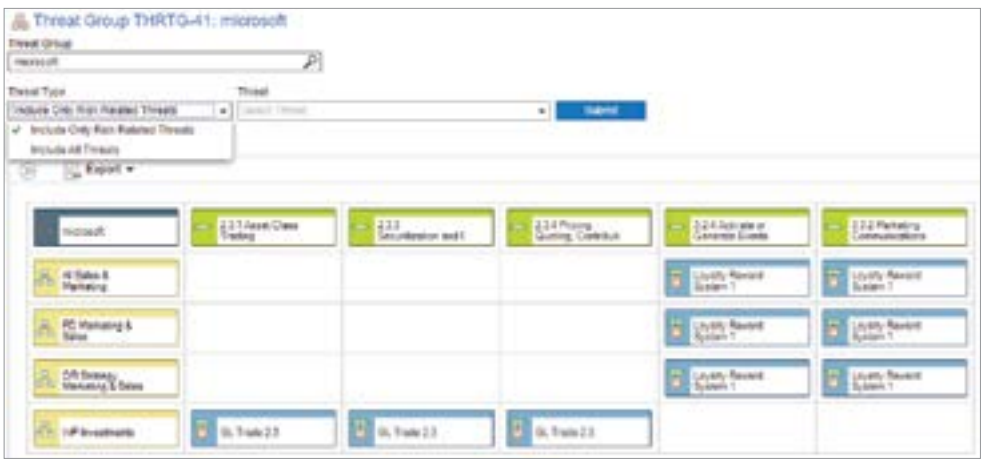

Figure 4: Business Support Map Indicating the Business Impact of Threats

Alfabet's solution for threat management has several key benefits

Best of both worlds
The threat management solution in Alfabet provides a unique combination of continuously updated content from one of the best repositories of vulnerability management data and a high-usability structure replete with ready-to-use explorers, workflows and business intelligence to manage this content effectively. Thus, enterprise architects, portfolio managers and S&R professionals can easily keep track of the growing number of vulnerabilities with a user-friendly medium.

Continuously evolving system
The system is standard enough to be used out of the box but using it over time makes it learn from past to present actions and manage the imported data that is relevant to your organization. It offers flexibility without customization. By grouping threats into various categories and understanding relevant threats to your IT landscape, threat management is much more simple and effective.

Readily available business impact information
The business impact of every threat and threat group can be made available through a business support map. Understanding the impact of the damages that can be caused due to the various threats helps gain a clear overall picture, vital for risk assessment. You can then easily classify and prioritize what threats or threat groups require immediate action and develop clear strategies to mitigate the associated risks.

Excellent follow-up capabilities
The system doesn't simply stop at documenting the threats, induced risks and their planned mitigations. Due to excellent internal integration with demand management and project management, it enables a detailed follow-up process to see how the planned mitigations are being implemented. This is a useful feature to catch risks at an early stage of a project, thereby minimizing potential loss.

Take the next step

For more information on how Alfabet can help you manage threats in the digital age, contact your Software AG representative or visit www.SoftwareAG.com/alfabet.

wp_alfabet_threat-management_en

software AG