ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 05(B), pp. 32229-32231, May, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A STUDY ON UNIFIED THREAT MANAGEMENT (UTM)

Mr. Ravindranath Mukhi, and Abhijit S Desai

Master of Computer Applications Bharti Vidyapeeth's Institute of Management & Information Technology, Belapur (CBD) India

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3426

ARTICLE INFO

Article History:
Received 12th February, 2019
Received in revised form 23rd March, 2019
Accepted 7th April, 2019
Published online 28th May, 2019

Key Words:

Network security, Chief Information Security Officer (CISO) , Unified ThreatManagement (UTM), Web Filtering

ABSTRACT

Unified threat management also abbreviated as UTM, is an approach to information or data security where multiple security threats or functions can be solved by a single capable security solution on the network.[1]43% of the 1,519 UK businesses that participated in the 2018 Cyber Security Breaches Survey from the Department for Digital, Culture, Media and Sport (DCMS) found that these businesses had experienced a cyber attack or security breach. The most prominent reason for the industry to be pushing towards unified threat management (UTM) is fines for major data breaches resulting in data loss and data tampering. The General Data Protection Regulation (GDPR) has driven several chief information security officers (CISOs) to re-evaluate their security posture. Organisations may have to face fines of 4% of their global turnover under the new data regulation, that was established in May 2018.According to Peter Wenham (Member of BCS Security community of expertise), UTM systems can help reduce the threats that could lead to a breach. [2]

INTRODUCTION

Throughout the evolution of networking and the Internet, the threats to information and networks have risen and widened dramatically. Security on the Internet and on Local Area Networks (LAN) is now one of the challenges for any organization. IT teams always have to confront the evolving and sophisticated threats, including spam and phishing attacks which endanger companies' productivity and digital assets on regular basis. They have to handle these challenges with restricted budgets and resources. Having multiple different devices, each designed to perform certain functions exclusively such as spam filtering, web filtering and antivirus protection make a whole lot difficult task to be done. Rather, it adds to the value and complexness of managing multiple boxes and multiple in operation systems.

UTM Could be a single System that has the Solution to all of the Challenges below and more:

1. It secures the network from viruses, malware, or malicious attachments by scanning the incoming data with the help of Deep Packet Inspection (DPS).
2. The packet headers of data are inspected first before allowing it to enter the network, thus preventing malicious attacks.
3. By installing enhanced web filtering, access to unwanted websites is prevented.
4. It provides ability to update automatically with the latest security updates, anti-virus definitions, and new features so that minimal manual intervention is required beyond initial set-up.
5. Management of wide range of security functions with a single management console through administrators is enabled by UTM.[3]

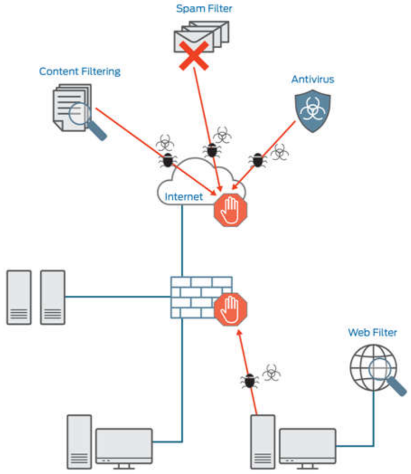

Figure 1 UTM Deployment in Network [3]

How UTM works and Deployed

UTM systems offer increased protection and visibility, in

*Corresponding author: **Mr. Ravindranath Mukhi**
Master of Computer Applications Bharti Vidyapeeth's Institute of Management & Information Technology, Belapur (CBD) India

addition as management over network security, reducing complexness.UTM systems usually do that via examination ways that address differing types of threats.

These Methods Include

Flow-based inspection, additionally referred to as stream-based inspection, samples information or data that enters a UTM device, then uses pattern recognition to work out whether or not there's malicious content within the data flow.

Proxy-based inspection acts as a proxy to rebuild the content coming into a UTM device, and so executes a full examination of the content to go looking for potential security threats. If the content is satisfactorily clean after inspection, the device sends this content to the user. However, if a malicious content or different security threat is detected, the device removes the questionable content, then sends the file or webpage to the user.

UTM devices offer a single programme for multiple network security functions and provide the advantage of single interface for those security functions, likewise a single purpose of interface to observe or analyze security logs for those completely different functions.

Businesses may implement UTM as a UTM tool that connects to a company's network, as a software system program running on existing server network, or as a service that works in a cloud environment.

UTMs are particularly useful in organizations that have many branches or retail outlets that have traditionally used dedicated WAN, but are increasingly using public internet connections to the headquarters/data center. Using a UTM in these cases offers the business additional insight and higher management over the protection of these branch or shops

Businesses can make a choice from one or additional strategies to deploy UTM to the suitable platforms, however they will additionally notice it best suited to pick a mix of platforms. Some of the choices embody putting in UTM code on the company's servers in data center; using software-based UTM products on cloud-based servers; using conventional UTM hardware appliances that come with preintegrated hardware and software; or using virtual appliances, which are integrated software suites that can be deployed in virtual environments.[4]

Benefits of UTM

UTM systems were designed primarily for small to medium-sized enterprises (SMEs), but suppliers are increasingly promoting UTM as a viable and beneficial option for large enterprises. The advantage of implementing a UTM appliance is that there is one interface from that we are able to manage both UTM appliance practicality and to look at network events throughout a consolidated view. Other UTM appliance functions will embody prioritising events and therefore the alerting of serious events via video screens, SMS text messages and email, in addition to comprehensive reporting capabilities.Some products also offer artificial intelligence (AI) to aid diagnosis of security-related events, while most offer tools toaid investigations.Web filtering is arguably the foremost powerful client-facing UTM tool which acts as a shield for the organisation.By intercepting web requests at the point of initiation and using predefined and frequently updated whitelists and blocklists of sites, an organisation can screen out and mitigate the threat posed by a significant proportion of phishing attacks, malware-infected emails and links, scams and other threats that could compromise user and data security. A centralised approach will counter any local client preferences or lapses in judgement and best follow. Thus, it can restore the messaging signal-to-noise ratio to a level where email is a net benefit to the organisation, rather than having inordinate amounts of storage space and user time wasted on junk, scams, threats and similar security challenges.

To optimise the potential of a UTM system, that an organisation determines which of its functions to enable with reference to the threats faced by the business and whether the respective functions offered by the UTM system meet security and business needs.The performance of the UTM platform should also be tested prior to adoption to ensure it has the capacity to handle the loads that existing and new features can generate.[2]

What are you protecting ?

“It is vital before buying any security system is to first establish what you are protecting, why, and from what you are protecting it. Seems basic, but you would be amazed at the thought that sometimes fails to go into this part of a specification. For it to be the right tool for the job, you need to know what the job is,” says Mike Gillespie, vice-president of the C3i Centre for Strategic Cyberspace and Security Science (CSCSS).

For a complete network redesign of associate existing infrastructure, there's bigger scope in UTM tool choice, from on site UTM network appliances to outsourced cloud-based services, or a combination of approaches. Such a redesign should lead to an optimal solution for an organisation, but would typically cause major disruption while being implemented.

Updating existing infrastructure involves exchanging existing infrastructure devices with a UTM appliance that gives wider capabilites and either one unified management interface or implements a software-based central management system providing UTM capabilities. A basic approach to UTM could be to replace a firewall with a UTM appliance offering a firewall with intrusion detection and intrusion prevention.
But implementing a UTM appliance with many functions may require a partial redesign of an organisation’s infrastructure.[2]

Security Failure

With a UTM, there's single point of failure within the company IT security systems.While you may have combined several functions into one platform, you are relying on all of those functionsbeing carried out as efficiently as a single function offering could do.Therefore, it is as sturdy as it's weakest element.

Organisations need to plan how to deploy UTM to establish a security architecture based around the security principle of defence in depth by using technology from a variety of suppliers and manufacturers. As an antidote to UTMs becoming a single point of failure, enterprises are encouraged to implement paired devices, ensuring high availability.It is imperative to understand that a UTM by itself is only one part of the puzzle and needs to be part of an overall security strategy, especially considering that a host of new technologies that are being adopted by enterprises bring their own challenges.[2]

Manage Expectations

We need to manage our own expectations of what a UTM can and can't do, as well as knowing what we need it to do. There is no purpose of changing a number of unnecessary security solutions from a variety of suppliers with variety of unnecessary security solutions from one supplier.We need to make sure that we have the skills, plan and team in place that are able to act on intelligence that UTM systems generate and ready to make the most of that insight.

Like all security technologies, UTM is constantly evolving, where businesses are under immense pressure to disclose breaches. The ability to forensically report on attacks will be key.UTM can be a useful tool to enable businesses of all sizes to strengthen their data protection capabilities by providing a consolidated view of what is going on in the network, however UTMs alone cannot solve all challenges regarding data protection.

Unified threat management tools should be carefully hand-picked and tuned to satisfy the data protection needs of the particular business, and care must be taken to ensure that a UTM does not represent a single point of failure byincorporating it in a robust, multilayered security architecture. An analysis of the pros and cons in the context of the organisation must be conducted before implementation and on anongoing basis to ensure that the UTM continues to meet the organisation's requirements.[2]

UTM is not a silver bullet

Over-reliance on a UTM system must be avoided, in other words, using UTM shouldn't mean foregoing controls at other levels throughout the organisation.UTM systems depend on large amounts of saved data to observe patterns over time as well as determine immediate threats. When implementing UTM, the team should perceive the data necessities, convenience of storage and potential impact on key applications before installation.

Cyber security processes are undervalued in the portfolio of security programmes. Cyber security should start with processes at the beginner level – once these are implemented to a satisfactory level, add more advanced processes.

Companies place numerous technologies in place, in some cases implementing these while not looking after how they'll be managed, monitored and integrated into the remainder of processes.[5] UTM or any other technology for that matter, isn't suitable in the absence of well-executed processes. Starting with the critical controls implemented as processes, supported by trained people, good configuration and managed technologies. It is only then there is a realistic chance to protect against data breaches.[6]

CONCLUSION

As threats continue to evolve, therefore too can UTM tools.UTM tools will become more expansive as they cover the ever increasing attack vectors available to criminals. They will also look at offering protection at a deeper network level to cope with the plethora of devices now connected to the internet. Ultimately, UTM systems – like all sorts of threat prevention – can continually be in responsive mode, chasing the newest threats and adapting consequently. To that end, it'll still need the guile of a strategic CISO (Chief Information Security Officer) to know their own network, determine the weak points, and deploy tools suitably. Whether that's a UTM system, bespoke tools, or combination of the two, nothing will beat the strategic outlook of awell-versed CISO.

The threat landscape has exploded due to the web and services designed on web technologies gain in acclaim. Given that every device – whether it is a corporate PC, a smartphone or an internet of things (IoT) device such as an internet-connected TV or security camera – requires an open connection to the internet, this provides a network port through which hackers can target attacks.

Understanding the health of the corporate network from a security standpoint – where are attacks being targeted orwhich exploits have broken through – is key to stopping or limiting damage from any attacks.UTM may go some way to helping security admins manage the ever-changing threat landscape by providing a single console to assess the overall security posture of the corporate network.

References

1. https://en.wikipedia.org/wiki/Unified_threat_management
2. https://www.computerweekly.com/feature/Making-unified-threat-management-a-key-security-tool
3. https://www.juniper.net/us/en/products-services/what-is/utm/
4. https://searchsecurity.techtarget.com/definition/unified-threat-management-UTM
5. https://www.computerweekly.com/opinion/Security-Think-Tank-No-tech-will-ever-counter-balance-poorly-implemented-processes
6. https://www.computerweekly.com/feature/Layer-your-approach-to-web-security

How to cite this article:

Mr. Ravindranath Mukhi, and Prof. Abhijit S Desai., 2019, A Study on Unified Threat Management (Utm). *Int J Recent Sci Res.* 10(05), pp. 32229-32231. DOI: http://dx.doi.org/10.24327/ijrsr.2019.1005.3426