SIMPLY SECURE

G DATA WhitePaper

Layered Security

G DATA Software AG | March 2017

Contents

Introduction

As threats to digital business processes are evolving, only a comprehensive security concept can sufficiently protect all workflow stages. Layered Security includes traditional antivirus and other client-based protection mechanisms but also addresses other risks, such as workflow disruptions or even complete infrastructure outages. This paper will discuss the various types of risks that digital enterprises face as well as the protection layers that should be deployed as part of a Layered Security concept.

1. Risk categorization

The mission statement of IT administrators is to ensure that digital infrastructure reliably enables productivity. In that context, security software is a means to an end, not a goal in itself. Administrators should make sure that they know which risks their infrastructure faces and deploy appropriate solutions to mitigate those risks. To get an overview of threats to digital business processes, various types of risk categorization can be carried out. Depending on company and infrastructure size, risk management can and sometimes must be formalized using a standardized framework, such as ISO 2700x, PCI DSS or Common Criteria. Although not intended to replace a complete security and risk management strategy, intention-, asset- and impact-based approaches can help recognize risks and initiate the development of appropriate security concepts.

Figure 1: Risk categorization

Not every incident that affects an enterprise is the result of deliberate planning by an adversary. Categorizing risks by looking at intention has the advantage of directing attention to IT infrastructure threats that might otherwise be overlooked. Nature, for example, is one of the major unpredictable factors: a thunderstorm or excessive rainfall can cause immense damage to IT infrastructure, without any deliberate cause. There is a plethora of other risks that can also unintentionally have a large impact on daily workflows, such as bugs in third party components, configuration mistakes or unintentional data removal.

A different way of looking at risk is analyzing it at the asset level. Every digital business process involves one or more types of assets, such as hardware, software, data and personnel. Each of those categories can be broken down in subcategories representing risks. For example, for hardware assets, areas of risk include availability, protection against abuse and performance, whereas data risks need to be analyzed in terms such as backups, privacy and protection against unauthorized access.

The potential impact of risk scenarios is often hard to calculate. Nevertheless, it is important to analyze what-if situations in order to find out which risks have the highest impact and need to be

addressed with the highest priority. The impact depends on the type of company, its workflows, its infrastructure and many more factors, but can usually be expressed in one of a number of “currencies”, such as time, money or trust. These are not mutually exclusive. For example, incidents that cause infrastructure outage not only cost time but through productivity loss also influence finances. For enterprises whose processes are part of a digital value chain, such as an online shop, the potential impact of infrastructural issues is even larger. And with data protection legislation such as HIPAA and HITECH becoming ever stricter, a loss of confidentiality can have possibly fatal consequences.

2. Layered Security model

As risk analyses show, risks and risk types are manifold. However, typical security software only stops whichever specific threat it was developed to stop. To ensure employee productivity and guarantee infrastructure availability, solutions must cover a wide range of possible risks. Instead of just using a single type of protection, modern solutions need to consist of multiple modules that cooperate to offer so-called Layered Security.

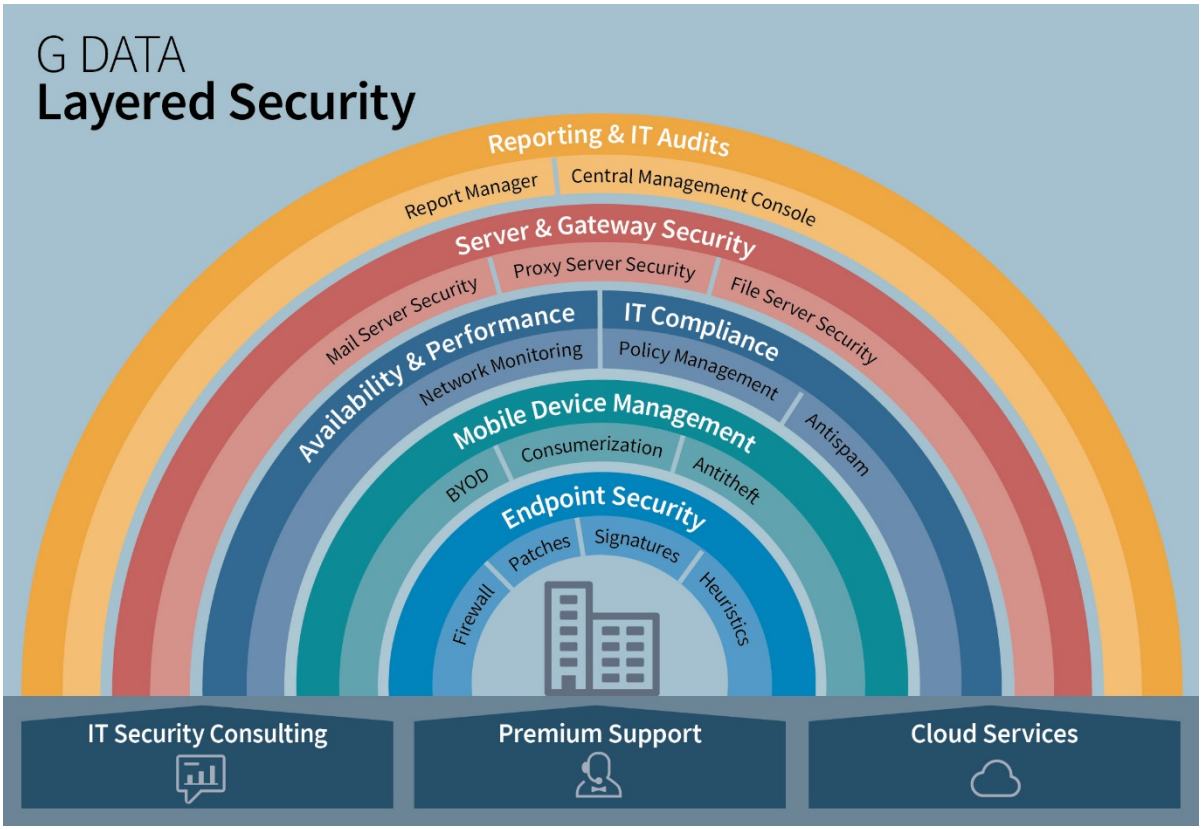

Figure 2: Layered Security model

The Layered Security model supplements traditional security components with technologies that address other risk types. A full-fledged layered concept does not just provide security on the server and endpoint level, but also guarantees availability, performance, productivity, data security and confidentiality, as well as offering services that complement every layer.

2.1. Endpoint Security

Like Layered Security does for network infrastructure as a whole, Endpoint Security itself also consists of multiple components. It unifies modules that complement each other and prevents the single point of failure that exists when relying on a single security technology. In the context of Layered Security, it offers an optimal combination of protection modules, whether securing desktops or laptops.

2.1.1. Firewall

Firewalls stop unauthorized traffic at the earliest possible stage. On the network layer, packets that are sent from the internet to an endpoint are either passed on or dropped, depending on the network security rules that have been defined. Firewalls also control traffic on the application level. This allows for a more granular control, enabling specific security policies per application, port or traffic type. Additionally, this approach ensures security even when the device is being used outside of the corporate network. When using a corporate laptop on a different network, using a client firewall will ensure that the level of security remains identical compared to the corporate network.

2.1.2. Patches

Vulnerabilities are discovered regularly in operating systems and applications, ranging in severity from allowing denial of service attacks to remote access or even remote code execution. Even though software vendors are aware of those problems and make patches available, it does not mean those are swiftly applied. In the period between a vulnerability being discovered and a patch being released and deployed, malware is often already exploiting the vulnerability. As soon as a patch is released, the affected component should therefore be updated as soon as possible. Deploying patches is essential to permanently mitigate software vulnerabilities, but also makes sure that applications are always performing optimally, for example by fixing compatibility issues and adding or extending features. Due to the sheer number of patches and the effort of testing and deploying them, it can take days or even weeks after a patch is released for it to be implemented, if at all. That is why it is strongly recommended to use a centralized patch management solution, which supports information gathering, tests and deployment.

2.1.3. Signatures

Signature-based detection is one of the oldest methods of finding viruses. Malware is detected by comparing files against signatures of known malware using statistical methods. When a match is found, the file is deemed malicious and can be blocked, cleaned or removed. Signature-based detection offers a high-performance detection of the large amount of known malware and thus forms a crucial part of the layered security concept.

2.1.4. Heuristics

Whereas signature-based detection requires signatures to be created from previously known malware samples, heuristics are based on general characteristics of malicious files. For example, even if a virus is so new that no signatures are available yet, heuristic detection could detect it based on its file header or other parts of the code. Heuristics make sure that viruses are detected before they are run, even if no specific signatures have been made available yet.

Like heuristics, behavior-based technologies also stop malware without relying on predefined signatures. However, unlike heuristics, they rely on malware's attempted actions instead of its file or code-based characteristics. Malware tends to act in distinct manners. For example, to ensure persistence, many types add entries to the registry or copy themselves to specific locations. Others download a malicious payload from an online server or access suspicious memory locations. Behavior-based technologies pick up on typically malicious actions and stop the culprit before it can do any damage. Some implementations provide general-purpose behavior detection, while others focus on specific usage scenarios such as online banking or ransomware threats. All have in common that they do not rely on predefined signatures or characteristics, allowing them to detect even previously unknown threats.

2.2. Mobile Device Management

Since smartphones and tablets have taken the world of consumer electronics by storm, the technology landscape has become a lot more complicated. Trends like the Consumerization of IT and Bring Your Own Device have introduced device diversity to the enterprise. Administrators are left with the task of providing broad access to resources while guaranteeing security. Mobile Device Management integrates this device diversity into existing administration workflows and helps optimize the efficiency of device deployment and management. Typical components include malware protection, theft detection technologies and device policies.

2.3. Availability & Performance

IT infrastructure needs to be run securely, but that is not the only factor to be considered. As IT has become a major pillar of doing business, its availability also has to be guaranteed. Performance loss and downtime directly influence business continuity. Internally, employees need IT infrastructure to be available whenever they need it in order to avoid loss of productivity. Externally, business partners and customers rely on web shops, communication systems, APIs and other IT infrastructure, causing revenue loss in case of downtime. To ensure availability and performance, Layered Security encompasses monitoring components. By keeping track of past and present performance statistics and availability metrics, monitoring functions as an early warning system that helps prevent infrastructural issues.

2.4. IT Compliance

Email, browsing, software – they are all parts of regular business workflows. However, without controls in place, improper usage of IT services can harm employee productivity. Using network-

wide policies, it should be made sure that internet access in general as well as specific applications are only available to the users that need them. Productivity can also be harmed by external factors, most notably spam. As a percentage of worldwide email traffic, spam consistently accounts for more than half of messages received. To make sure that unsolicited messages do not influence infrastructure performance and employee productivity, server- and/or client-side spam filters should be deployed.

Ensuring information confidentiality is key in safeguarding trade secrets, negotiations and product developments. The key feature of IT infrastructure, namely the efficient distribution of information, needs to be controlled to make sure that no confidential data leaks. For example, the use of USB sticks to quickly transfer documents between computers has to be limited in environments where sensitive data such as financial transactions or medical files is handled. Similarly, the use of software applications needs to be regulated in order to prevent confidential files from being distributed by email, instant messaging and the like. Data may be lost even without malicious intent. Hard disk failure or accidental removal of files can severely affect business continuity. Especially for businesses that are subject to privacy legislation such as HIPAA or security policy frameworks such as PCI DSS, a robust data security and backup concept is required, preventing problems and guaranteeing quick response and recovery times in case of emergency.

2.5. Server & Gateway Security

Before traffic reaches an endpoint, its content is often processed by one of the servers that are typically hosted within enterprise networks, such as mail servers or proxy servers. Those servers should make sure that unwanted content is filtered out at the earliest possible moment in time. For example, mail servers such as Exchange, Sendmail or Postfix can use plugins to scan email for spam or malware before delivering it to the endpoints. Similarly, web gateway servers such as Squid can secure web traffic using antivirus, antispam or antiphishing technology before forwarding it. Server and gateway security thus complements the use of a firewall. Whereas firewalls broadly allow or deny traffic based on predefined connections rules, server and gateway security analyzes the content of the traffic. File servers such as SAMBA should be protected as well, to prevent them from being used to distribute malware from an infected client across the network. Server security is also essential when the server forwards traffic to clients that are not protected by an endpoint module. When unmanaged clients, such as private smartphones or guest devices, connect to the corporate network, server-based components make sure even those are secured. Server and gateway security modules themselves can be layered as well, consisting for example of cloud, heuristic or signature-based components.

2.6. Reporting & IT Audits

Mitigating infrastructural risks such as security, availability and performance is not an install-and-forget process. Although many of the Layered Security components run independently, administrators should stay informed and ensure that they have access to the latest information at all times. The Layered Security model therefore explicitly defines Reporting & IT Audits as an independent layer. It should provide administrators with customizable reports as well as event and

alarm notifications, without generating too much “noise”. Administrators should also be able to quickly and easily find out which configuration applies to which network components and which modules urgently need attention. Ideally, an integrated management console provides functionality to configure all layers, while striking the perfect balance between configurability and ease-of-use.

2.7. Consulting, Support and Cloud Services

In addition to the individual protection levels of the model, Consulting, Support and Cloud Services span across all layers. For example, cloud-based technologies provide reputation lookups and other supporting information to various security layers. Services encompass management and configuration – for instance, for enterprises without dedicated IT personnel. Managed service partners can offer security solutions to businesses of any size, taking care of infrastructure management and configuration. Finally, incident response and consultancy services can help organizations set up and maintain security policies and handle malware incidents.

3. Choosing a layered security solution

Many networks are protected by security solutions that were installed successively as separate components. Even if they represent all important security layers (which is usually not the case), they only rarely cooperate. Using such a fragmented Layered Security concept makes the infrastructure more susceptible to configuration errors (and the resulting security issues) and increases the amount of time required for configuration and maintenance. Instead, it is recommended to implement all security layers as an integrated solution, which contains all necessary components and offers unified management using a single interface paradigm. The different layers should provide the best possible holistic security without sacrificing performance, manageability or efficacy. Moreover, when deploying an integrated solution from a single vendor, there is often a financial advantage compared to purchasing individual components.

Before choosing a specific solution, administrators should find out which parts of the infrastructure need to be secured and which risks apply (see chapter 1). When using risk management tools, they can be used as a basis for choosing a security solution. Alternatively, a list such as SANS CIS Critical Security Controls, which contains recommended defensive security components, can be used to prioritize and plan the implementation of Layered Security[1]. The prospective solution should not only cover all risk types and security layers, but also take into account endpoint diversity. Security layers such as signature-based detection or heuristics should be available for all endpoint types (such as Windows, Mac and Linux clients and servers). Mobile device management needs to be implemented to make sure that Android or iOS endpoints are also used securely and in line with corporate policies. Setting up one or more server- or infrastructure-based security layers, such as network monitoring, helps cover a large number of endpoints at once and addresses issues such as availability and performance.

[1] See https://www.sans.org/critical-security-controls.

G DATA offers solutions that cover the full spectrum of Layered Security components and protect the complete network infrastructure, including a multitude of endpoint types as well as email, proxy and file servers. By combining the solutions with one or more optional modules, they can be tailored to fit any network and guarantee security, availability, performance, productivity and data confidentiality. G DATA also offers various services ranging from support agreements to full-fledged hosted endpoint security. Up-to-date information on all G DATA Business Solutions can be found at www.gdatasoftware.com/business.