The Triple-A approach to network security

Florian Malecki, International Product Marketing Director, Dell Networking Security

Abstract

How can IT decision makers know when their organization has reached a level of security that will protect from cyber-attacks while still empowering employees to do their job better? This business brief explores the three essential factors that encompass a comprehensive security approach. Organisations whose network security rates high on all three factors deserve a triple-A rating.

Introduction

Triple-A (AAA) ratings are normally associated with Chief Financial Officers (CFOs) keeping tabs on bond or credit ratings. In the world of IT however, how can a CIO or IT decision maker (ITDM) rate the efficiency of an IT security implementation?

IT security is one of the main concerns for ITDMs because of recent vulnerabilities such as Shellshock and Heartbleed and others affecting organisations globally. Therefore, ITDMs are taking steps to protect the corporate network from threats of all sizes. However, as it stands, security is still at risk from internal and external factors.

How can ITDMs know when they have reached a level of security that will protect from cyber-attacks while still empowering employees to do their job better? A comprehensive security approach should encompass three factors:

- It should be **adaptive** to threats, business requirements and the ever-evolving use of the internet within the corporate network.
- It should have **adapted** to meet the specific requirements of an organisation.
- It should be **adopted** fully by end users.

A security approach is nothing without a security infrastructure to match. When implementing any new solution into the security portfolio of your network, it is essential to ensure the vendor is positioned to promote your organisation's growth with the solution. As I like to say; "Better security, better business!"

In fact, 73 percent of organisations globally have experienced a security breach in the last twelve months.

These factors can be summarised as a Triple-A security approach. If you achieve this, then you can strengthen the overall security posture and grant your organisation a Triple-A security rating. Read on to find out how you can achieve a security approach worthy of Triple A status and learn how IT security can be a driver of innovation, rather than an obstacle to it.

Adaptive

IT infrastructures are constantly changing. In the past we had static IT infrastructures; however, we are moving towards a world of convergence. Therefore, security infrastructures need to adapt to be effective. An adaptive security architecture should be preventative, detective, retrospective and predictive. In addition, a rounded security approach should be context-aware.

Gartner has outlined the top six trends driving the need for adaptive, context-aware security infrastructures: mobilization, externalization and collaboration, virtualization, cloud computing, consumerization and the industrialization of hackers.[1] But what exactly does context-aware mean? Gartner defines context-aware security as "the use of supplemental information to improve security decisions at the time the decisions are made," and predicts that by 2015, 90 percent of enterprise security solutions deployed will be context-aware.

The premise of the argument for adaptive, context-aware security is that all security decisions should be based on information from multiple sources. This starts by looking at the context of the request and then allowing or denying it based on the information available; for example, the method of authentication used, the time of day, etc. By taking this adaptive approach, security can be improved.

Adapted

No two organisations are the same, so why should security implementations be? Security solutions need flexibility to meet the specific business requirements of an organisation. Yet despite spending more than ever to protect our systems and comply with internal and regulatory requirements, something is always falling through the cracks. In fact, 73 percent of organisations globally have experienced a security breach in the last twelve months, according to a Dell-commissioned survey by Vanson Bourne.[2]

There are dozens of "best-of-breed" solutions addressing narrow aspects of security. Each solution requires a single specialist to administer the software and leaves gaping holes between them. Patchwork solutions that combine products from multiple vendors inevitably lead to the blame game.

There are monolithic security frameworks that attempt to address every aspect of security in one single solution, but they are inflexible and so expensive to administer that organisations often find that they become too costly to run. They are also completely divorced from the business objectives of the organisations they're designed to support.

Instead, organisations should approach security based on simplicity, efficiency, and connectivity, as these principles tie together the splintered aspects of IT security into one integrated solution capable of sharing insights across the organisation.

[1] *Neil MacDonald, Peter Firstbrook, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," Gartner, Inc., 12 February 2014, https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection*

[2] *"Protecting the organization against the unknown," Vanson Bourne, February 2014, http://software.dell.com/documents/protecting-the-organization-against-the-unknown-whitepaper-27396.pdf*

This means that business users can manage the rules and policies, and end users can easily comply. This type of solution ensures that the security approach has adapted to meet the specific requirements and business objectives of an organisation, rather than taking a one-size-fits-all approach.

Adopted

Another essential aspect to any security approach is ensuring that employees understand and adopt security policies. IT and security infrastructure are there to support business growth — an example of this is the way in which IT enables employees to be mobile, thereby increasing productivity. However, at the same time it is vital that employees adhere to security policies and access data and business applications in the correct manner. If they do not, then mobility and other policies designed to support business growth become a security risk that could actually damage the business.

People often think security tools hamper employee productivity and affect business processes. In the real world, if users don't like the way a system works and they perceive it as getting in the way of productivity, they will not use it. The business value of the system then disappears, not to mention the network security.

With mobility, for example, BYOD is one of the most common ways in which employees can make their organisation vulnerable to attack. Although BYOD has given employees an increased level of flexibility, it has also given the user even more potential to cause security breaches. In fact, data loss on mobile devices is considered a top concern for companies today with 71 percent of UK businesses citing "increased use of mobile" as a top threat to their IT security in the next five years.[3] To some extent this explains why some companies in the UK are reluctant to enable workers to access company networks using personal devices. In fact, 24 percent of UK respondents said less than a tenth of employees use personal devices, which is lower than the global average of 13 percent. Therefore, it is more important than ever to fully educate employees about security attacks and protection.

Providing employees with training and guides around cybersecurity should lead to fully adopted security policies, and the IT department should notice a drop in the number of security risks from employee activity.

Triple-A

If your overall security policy is able to tick all of the three A's, then you have a very high level of security. However, the checks are not something that you can do just once. To protect against threats, it is advisable to run through this quick checklist on a regular basis to ensure that a maximum security level is achieved and maintained at all times. It is also important to ensure that any security solution implemented allows your organisation to grow on demand, with no impact on the existing part of the network.

Overall, the Triple-A rating is a widely respected and trusted scheme outlining the financial status of a company or country. However, the Triple-A security test is also a good way to assess a corporate security network. By ensuring that the network is rated Triple-A, it becomes possible to ensure that all areas of a corporate network are protected at all times.

By working towards this framework, it becomes possible to identify gaps in network security, helping to prevent against future attacks.

71 percent of UK businesses cite "increased use of mobile" as a top threat to their IT security in the next five years.

[3] Warwick Ashford, "Businesses ignore unknown threats despite cost, study shows," TechTarget/ComputerWeekly.com, 20 February 2014, http://www.computerweekly.com/news/2240214754/Businesses-ignore-unknown-threats-despite-cost-study-shows

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.