TechTarget | Custom Media

Cyber Security Essentials for the Digital Infrastructure

In the age of digital business, companies of all kinds are facing a new and complex array of cyber security challenges. Today's threats are aimed at an IT infrastructure that includes not only the data center, but also public cloud services, high-speed networks and a host of diverse endpoints, including BYOD and Internet of Things (IoT) devices. IT leaders must secure sensitive data across this extensive landscape, while meeting increasingly stringent compliance guidelines. A comprehensive, disciplined approach is required.

Cyber security challenges

With attacks including virus, ransomware and denial-of-service multiplying in number and sophistication, the challenge of keeping data secure is more difficult than ever. Attacks come from both inside and outside the organization, from malicious hackers, nation-states, disgruntled employees and even trusted employees who unwittingly bring malware-laden mobile devices into a corporate facility, thereby exposing an entire organization to attack.

Because sensitive and valuable data continues to be stored and processed in corporate data centers, those facilities continue to be a target of thieves and malicious actors. Ransomware attacks, such as the recent WannaCry outbreak, cause data to be encrypted unless ransom is paid to the perpetrator. Denial-of-service attacks, such as that launched by the Mirai botnet in 2016, can bring down data centers and networks. Mobile devices represent a weak link

Sponsored by vmware

Table of Contents:

that is being targeted with increasing frequency. Not only is it relatively easy for the laptops, tablets and smartphones of BYOD users to be compromised through insecure Wi-Fi networks, thieves are well aware that a single stolen laptop can yield millions of valuable records.

Regulatory guidelines, such as the Payment Card Industry Data Security Standard (PCI DSS) in financial services, Health Insurance Portability and Accountability Act (HIPAA) in health care and the European Union's General Data Protection Regulation (GDPR), raise the stakes for cyber security. In addition to the financial losses resulting from data theft, non-compliance with regulations can be punished by stiff penalties. In the case of GDPR, organizations doing business with European customers must notify them within 72 hours of a data breach, or face fines as high as $4 million or 20% of annual revenues.

Against this array of threats and compliance mandates, such lapses as easy-to-guess passwords, sluggishness in applying security patches and misplaced devices must be avoided, at the risk of catastrophic consequences.

Cyber security essentials to-do list

IT leaders should follow a list of actions that includes responses to every security threat. Because attacks can come from anywhere, at any time, the practice of regarding all devices and individuals as untrusted is an essential starting point for all security measures. These include:

1. Securing access. The way that users are identified and granted privileges to access and manipulate data is made up of these elements:

- **Passwords.** Passwords should use two-factor authentication or be discarded in favor of biometric identification or cryptographic keys.
- **Least-privileged access.** Policies should enable only the access that is consistent with the role of a given user.
- **Validate, check and remediate.** The integrity of data must be validated regularly. Systems should be checked for breaches and remediated as quickly as possible.
- **Analytics.** Analyzing IT infrastructure information such as log data can enable an administrator to spot developing threats before they result in breaches.

2. Endpoint and IoT security. A diverse array of BYOD devices and new IoT devices such as factory floor sensors require a new level of vigilance. BYOD devices may contain personal as well as corporate information, they may connect to insecure networks outside the organization and

they may travel throughout the world—all of which increase the chances of compromise. IoT devices may not be secure and they may not be upgradable with security patches. Consequently, the zero-trust principle must apply to all endpoints. Encryption of data on endpoint devices, and while traveling over networks, is an essential defensive tool.

3. Networking security. Once confined within a building's walls, the network perimeter has changed dramatically due to the widespread use of cloud-based services as well as the proliferation of BYOD and IoT endpoints. To meet these challenges, data should be encrypted both in motion and at rest. When virtualization is deployed, micro-segmentation should be implemented in order to isolate a security compromise to the segment in which it occurs. In addition, automation should be utilized wherever possible. For example, rather than sending an alert—which might be ignored by an administrator—it is more effective to block suspect actions on the server and remediate them automatically, while allowing an administrator to conduct a thorough investigation later.

4. Data center security. In the data center, workloads and applications are increasingly virtualized, achieving greater server utilization and lowering total cost of ownership. Applications running on virtual machines in the data center should be secured using encryption, threat detection, data protection and network security. When an application is moved from one virtual machine to another, these security measures should move along with it. On the desktop, end-user systems can be virtualized through virtual desktop infrastructure (VDI) technology. Under VDI, applications and data remain on a server while the user interface is displayed on the client system. VDI can enhance security be keeping critical data off end-user devices. The enhanced security afforded by both server and desktop virtualization is beneficial for regulatory compliance.

5. Cloud security. The use of cloud-based services is widespread across organizations of all kinds. Just as in the data center, it is important to gain insights into the security of data in the cloud, and to be able to validate the security and compliance of cloud-based data. In addition, it is important to know where in the cloud data is stored. The data sovereignty regulations of some governments may mandate that data never leave a given country. Data pertaining to citizens in EU countries must be stored in compliance with GDPR guidelines. Because organizations often move data between cloud services and on-premises data centers, the best approach to cloud-based cyber security is to utilize a common platform that supports both on-premises data centers and cloud-based services.

6. Compliance. The rise of regulations means organizations that are victimized by a breach must pay severe fines. Guidelines such as PCI DSS and HIPAA have been in place for years. Meanwhile, GDPR's severe penalties for non-compliance become effective in May 2018. Because compliance touches many parts of IT infrastructure, it should be addressed in all parts of this to-do list. Encryption is a critical compliance tool, and should be implemented for sensitive data wherever possible.

7. Technology integrations. The new difficulties in bringing about cyber security in the era of digital business require an integrated solution. Implementing one security technology for endpoints, another for servers and storage, and yet another for networks might keep data safe, but at a tremendous increase in complexity and cost. A far better approach is a comprehensive solution in which security technologies are designed to work together throughout the enterprise. The integration of network and endpoint security in particular has the potential to reduce total cost of ownership and improve threat detection.

Conclusion

As digital strategies have changed the business landscape, IT infrastructure has changed to include not only on-premises data centers, but cloud-based services and a broad array of endpoints, including BYOD and IoT devices. In addition, regulatory compliance requirements are a fixture in several key industries, even as GDPR emerges as a hurdle for global organizations. In this landscape, enterprises that approach the cyber security issues of identity, mobility, virtualization, cloud, and regulatory compliance in a comprehensive and integrated manner are likely to achieve their security and compliance goals, while simplifying complexity and controlling cost.

For more information, please visit http://vmware.com/go/cybersecurity