Summary Insights: Shoring Up Cyber Defenses

RFG Perspective: Shoring up cyber defenses must become an urgent priority for organizations given the heightened threat of a global cyber warfare. As the theater of war evolves in Ukraine, DDoS and ransomware offensives may increase – whether sourced from Russia, its allies, and other state actors that might increase their attacks on Western governments and organizations by employing cyberattacks. Following the Russian invasion of Ukraine, some published reports claim we are already seeing attacks on American banking institutions up more than two-fold.

In the same vein that traditional battles employ the use of structurally damaging armament against opposing forces, cyberattacks allow nations to impose their will by destabilizing essential institutions, including financial systems and governments, and key infrastructure networks. Should the physical war in eastern Europe escalate, it should be assumed that European and U.S. systems supporting financial and infrastructure (e.g., electric utilities) would rank highly on the intended target list. It is therefore imperative for enterprises to assume both preventative actions and remediative postures in the event that any future breaches succeed.

Last year, President Biden issued an executive order instructing government agencies and private organizations to prepare for state-driven cyber menaces by addressing lapses in their cyber defenses and by enacting plans to minimize impacts of any successful penetrations.

The war in the Ukraine and the President's executive order are adding extra impetus for enterprises to determine what their cyber gaps are – and what actions they can take to shore up their cyber exposures. These actions should encompass the closure of entry points, and measures that would minimize the blast exposure if an enterprise's defenses failed.

On Mar. 9, 2022, the Robert Frances Group facilitated an RFG 100 videoconference entitled: **"Shoring Up Cyber Defenses."** This videoconference delineated what the participants believed to be the key exposure areas and actions that executives should take to minimize their cyber risks.

The panelists for this video conference were:

- Rob Bathurst, CTO, Epiphany Systems
- Eric Herzog, CMO, Infinidat

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

- Ev Kontsevoy, CEO, Teleport
- Kaustubh Medhe, head of research and cyber threat intelligence, Cyble

Poll

A quick poll of the attendees on this topic yielded the following results:

- 42% of respondents felt their organization could recover from a 30-day long ransomware attack (from inception to point of discovery or shutdown) while 33% were unsure whether or not they could recover. Only 17% of respondents were confident they could be back in operation within hours.
- 33% of respondents stated that their organization could recover from a ransomware attack lasting 180-days, or longer, while 17% believed they could not recover from such an attack, and 50% said they were unsure.
- 83% of respondents were satisfied that their organization could fend off a DDoS denial-of-service attack. The remainder of the respondents were unsure of the organization's ability to respond to the attack.

Defense in Depth

Panelists hammered home the point that enterprises needed to have a defense in depth plan in place and executed — to protect against cyberattacks and ransomware. They recommended that executives should use the military approach to defense, by deploying systems with multiple layers of protection. Executives need to know what resources are "of value" to attack – and what are the possible objectives of such an attack. This analysis needs to extend to the supply chain and to peer networks, from which an attack could begin. Then, executives need to determine how to prevent the cyberattacks, protect the target, and contain any breach of enterprise security.

Part of the analysis for containing the breach must include a determination of how quickly a containment plan can be executed – and how to reduce the blast radius to an optimal minimum impact level. This will require building out attack chains and knowing who in the organization has authentication rights and what the vertical stack for their organization's software looks like.

Panelists pointed out that frequently before an actual target is attacked, the initial target could be the degradation of the command-and-control structure of an enterprise – or even to take over the entire command-and-control structure. Thus, IT organizations must first ensure that they could repair and restore the command-and-control structure quickly, following an attack. This capability should be built into the IT architecture – it should not be an add-on. This has to be the second line of defense for corporate security, panelists said. Without a strong defense-in-depth posture, the organization's operations could cease to function for an extended period of time, damaging its reputation and its hard-won corporate brand.

Protect the Data

Since a successful ransomware attack blocks access to an enterprise's data, it is imperative that IT controls and protects both its primary storage and secondary storage.

IT organizations must be confident that they have created good, immutable copies of key data that cannot be changed, once stored – and they must make sure that they are creating newer copies of the updated data on a scheduled basis. Those datasets that are disposable or easily recreatable need not be copied for protection purposes. It is best to have these copies existing on a logical or physically air-gapped system and in a "fenced off" network that cannot be accessed from the outside. Panelists suggested that it would also be advantageous to ensure that there is a separation of the data and the control plane.

To minimize any gaps in the security perimeter, executives should ensure that ransomware and malware tests are done periodically. It was suggested that key datasets be profiled and scanned for malware weekly – or at least monthly. A catalog of these copies needs to be maintained, as well.

It was further recommended that enterprises practice for a typical disaster scenario, whether it be a flood, a hurricane, or a cyberattack. Today, most organizations do practice runs for disaster recovery and business continuity on a periodic basis. However, we should note that some organizations do not test on a regular basis. This is a situation that our previous polls have shown – even though building up security is more important than ever for cloud migrations, hybrid cloud and multi-cloud deployments.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

Enterprises should also practice for ransomware and malware continuity. If these recoveries are done on a regular basis, then the organization can create an index or catalog of known, good copies. If this is done correctly, the right application of software-based automation can make the creation of a catalog a seamless process.

Five Advantages for Monitoring the Dark Web

Monitoring the Dark Web can help to prevent breaches, as well as to reduce of the post-breach risk exposure. In terms of preventions, an examination of the Dark Web can help security teams to understand what vectors and attack types are currently most active – and to determine the source of the attacks.

Secondly, the security team can do an analysis of compromised credentials – such as VPN credentials, remote desktop credentials, active directory credentials, and email credentials – so that they can secure them or shut them down. This type of analysis is key, because studies show that nearly 70 percent of these breaches happen when threat actors gain entry into the enterprise environment by using a compromised credential.

One other factor to consider: There are underground forums on the Dark Web in which compromised cards, debit cards, credit cards, wallets, and banking accounts are available for sale. By monitoring the Dark Web, enterprises will be in a position to take remedial action – which could include locking or listing the cards, hot-listing the cards, disabling the accounts, or enforcing multifactor authentication (MFA) for these high-risk accounts. Any of these actions would reduce fraud loss or plug revenue leakage.

Knowledge of which attacks are in progress and their characteristics allows security teams to learn whether a similar attack could strike them and what the impact of such a strike would be. They can therefore be prepared to prevent such an attack – or if that is not fully possible – they can determine what could be done to reduce the response time and the associated costs. If one thinks about this chain of events as compromise of customer accounts, then it would be better to have an exposure of some of the accounts and to remediate that situation, rather than to address the breach of all customer accounts.

Lastly, by having a detailed knowledge of the cyber topology, one may be able to spot a breach quickly and thereby report the issue within the 72-hour compliance requirement. It should be noted that hackers usually log into systems – rather than breaking in. If the security team were able to learn the scope of data exposed quickly, then it could learn the total extent of the breach as part of a forensic review. This rapid-response capability not only enhances customer trust, but it also can reduce insurance costs, which are rapidly rising due to excessive losses.

Other Considerations

In most cases, breaches are an exploitation of a human error. This is used to gain entry into an enterprise's IT systems, inclusive of compute, networking, and storage capabilities. For example, 86% of respondents in a recent survey said that they could not guarantee that former employees would not be able to gain access to data inside of the enterprise's firewalls. In that scenario, the hacker would be able to pivot sideways to find his intended target.

Hackers can gain access through one of many entry points: applications, databases, Kubernetes APIs, or SSH dumps – or even snapshots of virtual machines (VMs) and data. Today's hackers and state-actors are very creative and are very persistent. They can access silos and then move into other systems while hunting for their planned targets. One challenge for enterprises is that they have multiple tools for cyber defense and analysis – and that many of these tools, and the data they manage, are siloed. Executives should consolidate them to the minimum amount possible.

Some possible remedies for protection include replacing passwords, using API keys, or using SSH keys with secretless access. The use of a Secretless Broker relieves the application from the need to directly handle corporate secrets. The Secretless Broker thereby prevents loss or theft of credentials and manages the ID certificates. Because there are potentially thousands of secrets within a global enterprise, this action alone could have a dramatic impact, by making the sale of security credentials valueless. By taking this approach, every human, machine and microservice would have its own ID certificate that meets enterprise security policies – and that expires automatically, so that administrators do not need to take actions to cancel it.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

Summary

Executives who are responsible for a P & L are traditionally more interested in keeping costs down than in worrying about future potential problems that may never occur. That is why it is imperative for IT leaders to make their colleagues, the business executives, aware of the corporation's vulnerability to cyberattacks and ransomware attacks. In short, that's why IT should perform a risk assessment before any new application or enhancement goes online.

In addition, IT should periodically provide a detailed defense-in-depth assessment and report its findings to senior managers, the CXO suite and to business executives throughout the organization. Even with excellent cyber defenses in place, IT should plan to protect the business against cyber breaches by prioritizing the creation of restoration lists for critical applications and databases. This list should prioritize what needs to be restored and operational within 24 hours and delineate what can wait longer, up to 72 hours from an attack.

RFG POV: Shoring up cyber defenses with a viable defense-in-depth plan is all about getting business and IT executives to agree on what constitutes an acceptable level of risk for the organization. A discussion of acceptable risk must cover both financial impacts and the impacts to the company's reputation, both of which will affect customers' faith and trust in the enterprise. *IT executives must remember that this is, fundamentally, a business risk discussion and not a technical issue.* In many cases, IT gets bogged down in its own jargon and concerns when explaining their security concerns to business executives. Unfortunately, in many cases, business decision-makers may not concur with IT regarding the overall business risk exposure, with the result that they will not fund the requested additional security precautions. In all cases, IT should document the issues, discussion, parties involved, and conclusions.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com