Security in computing environments in depth

Introduction

Previously, you found out about the fundamental security points in a computing environment that need to be considered when developing a security strategy. Specifically, a good policy should be able to stop unauthorized access, limit mobility within a system, and minimize any damage resulting from a breach. In this reading, you will learn more about the measures taken to enforce these points, with a focus on the following:

1. Preventing an attacker from gaining entry to a system.
2. Segregating a system so that the damage to a system once accessed is limited.
3. Best practices for storing copies of your system.

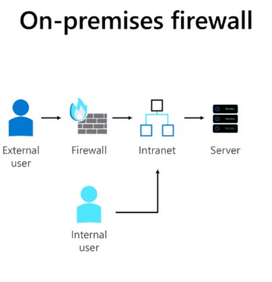
The policies and procedures you implement are your strategies for offsetting malicious manipulation from a would-be-hacker. Not having a plan is akin to planning to fail. Every organization needs to know how to prevent any malicious tampering and react at any breach stage. Finally, once a breach is complete, how to implement recovery as quickly as possible.

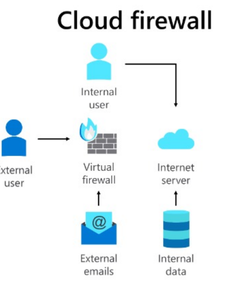
Currently, Sam only uses personal devices to access emails related to Sam's Scoops. She has taken some basic security measures and knows about best practices for staying safe. However, Sam is not sure if this is enough for a more complex business setup. Let's find out what Sam should know in order to develop an effective approach for protecting customer data.

Preventing an attacker from gaining entry to a system

Gateway security is the top recommendation for cybersecurity. The reason is simple: if you can prevent any external unauthorized entity from accessing your system, you can ensure that your assets are protected. As with personal computers, the devices for accomplishing this are known as a firewall. A firewall will sit between a trusted network and filter traffic coming from an untrusted one.

With on-premises access, implementing a firewall is relatively straightforward; all traffic coming from the internet is outside traffic and is treated with severe restrictions. All inside traffic is authorized and subject to more relaxed constraints. This is somewhat more complicated for cloud-based businesses, as the resources accessing the cloud resources may be dispersed. This means that it is more difficult to make a clear distinction between the inside and outside of a network.





Segregation to limit damage upon access

If a threat is able to breach a gateway, there is another safeguard that can be implemented:

Segregation access is an effective security measure that can be applied to both traditional and cloud-based businesses. There are several ways that this can be achieved, and later you'll learn about such concepts as identity management concepts and role-based access. For now, you only need to know that the shared idea is that access to one area only gives you a pass to some parts of a business, not all of it. These cloud-based solutions are implemented to deal with the vulnerabilities created by people accessing company resources using different types of devices in different and changing locations.

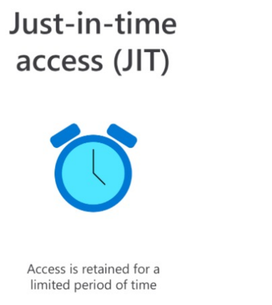
Zero Standing Access is the overarching concept that access to the production environment must be kept to a minimum and cannot be persisted over time. This means you must validate that you are authorized whenever you wish to access production-related areas. Even then, your access will only allow you to make changes sufficient to the area you have been authorized to access. Two critical policies that have grown from this are:

1. **Just-In-Time (JIT)**

2. **Just-Enough-Access (JEA)**

JIT means that having accessed a given area; you will only retain your access for a limited period of time before you are automatically ejected or asked to re-enter some authorization code. JEA relates to the limitations on the changes you can make while there. As a security specialist configures which areas should be accessed by which individuals, as well as what privileges are required when a specialized task needs to be engaged very carefully. Giving the wrong individual inappropriate access can be the difference between a minor and a severe security breach.

Consider this situation: Sam hires someone to clean the windows on the shop front. Rather than giving this person the keys to the safe; instead, Sam will make the window and all the required access to this window available to the cleaner for the duration of the cleaning. If this includes keys to the shop, those keys are returned at the end of the process and will not include a key that could potentially open a safe or cashbox.



Recovery

While the first two parts of cybersecurity concern keeping intruders out and minimizing damage, the third relates to a policy for undoing any harm that might have been caused. In this regard, cloud-based businesses have an advantage over traditional ones because creating back-ups and spinning up new environments is part of cloud computing.

In a traditional approach, applications are run on hardware, and it is advised to save and back up information regularly. Recall that this can be done by following the 3-2-1 recovery plan, which involves keeping three copies of everything in 2 formats, and 1 copy off-site.

In operating on the cloud, cloud-based businesses already have their workflow virtualized. In addition, the underlying architecture ensures that backups are created of everything that goes online. This ensures that if there is an issue with accessing a business's resources, the hosting company can provide an alternative. Finally, it is a good practice employed by cloud providers to store information in different geological locations (see the reading Azure Storage redundancy for more information).

Conclusion

In this reading, you learned about some of the specific methods and policies that both traditional and cloud-based businesses can implement to create a security strategy that will prevent access, limit exposure, and mitigate fallout.