T2023_01 How to find a balance between Security and Employee Trust (17th January 2023)

Difficulties with an enforcement-based approach

An enforcement-based approach to security begins with a security policy that is supported by security controls, which are frequently heavy-handed and aimed to prohibit personnel from participating in dangerous activity or unwittingly expanding an organization's potential attack surface.

Most firms only utilize enforcement-based security controls which are often implemented at the network level using a Cloud Access Security Broker (CASB) or a Security Services Edge (SSE). CASBs protect data in transit between on-premises and cloud architectures, as well as check authorization rules and access controls against the company's security policy. Some organizations employ CASBs to ban SaaS (Software as a Service) applications, however CASBs, like SSEs, only support a limited number of applications.

The applications that these technologies do not support are frequently the most dangerous since they do not adhere to common industry and security standards, such as SAML for authentication and SCIM for user management. These are referred to as "unmanageable apps,". Unmanageable applications are popular, and the rate at which employees buy and deploy them has hit a new high due to the post-COVID environments.

IT departments were primarily in charge of procuring and delivering enterprise-wide applications but the shift to remote work gave individuals across enterprises the ability to choose their own tools. This increases digitalization provides them with an ever-expanding set of tools to pick from, resulting in an explosion of unmanageable applications.

The ordinary user does not consider security first. Most individuals assume that programs are secure, and some may be unconcerned about security at all. Most consumers are concerned with user-friendly features, design aesthetics and ease. To suit these new objectives, application providers revised their product roadmaps; security was no longer a primary concern for many of them.

Unmanageable applications, whether employees are aware of it or not, can have a severe impact on an organization's security and frequently add to the workload of technology teams. Someone must keep an eye out for troublesome programs,

activate features like two-factor authentication (2FA) and enforce secure passwords.

Many organizations block or ban unmanageable applications to alleviate the pressure and it is easy to see why corporations embrace this approach: it is a rapid and consistent way to handle a pressing and worrying issue. A strictly enforcement-based approach, on the other hand, is not sustainable or realistic in practice as a long-term, complete solution.

Advantages of an enrollment-based approach

An enrollment-based cybersecurity approach gives employees more flexibility, individualism, and choice. It encourages them to actively participate in enterprise-wide security and compliance activities. In contrast to enforcement-based systems, an enrollment-based strategy allows employees to choose whatever applications they want to use for work.

Establishing a balance is the best solution for both firms and people. Employees should be able to pick which programs they use, and companies should not be concerned about security.

When employees understand that application selection comes with responsibility and the necessary tools are easily available, security becomes everyone's priority. When self-enrolling and registering applications become available, the same employees who detest application choice policies will gladly accept easier and stronger security with the added benefit of compliance.

The Guyana National CIRT recommends that users and administrators review this tip and implement them where necessary.

References

- The Hacker News. (2023, January 4). *Enforcement vs. Enrollment-based Security: How to Balance Security and Employee Trust*. https://thehackernews.com/2023/01/enforcement-vs-enrollment-based.html