THE NATIONAL CYBERSECURITY SOCIETY

LEAST PRIVILEGE

HOW WILL LEAST PRIVILEGE PROTECT MY BUSINESS?

Least privilege is defined as giving a user only those privileges that are essential to perform his/her intended function. All companies, regardless of how large or small they are, must manage the access employees have to corporate assets. It's very easy for small companies to fall into the trap of thinking that they can just give everyone access to everything. It's quick, easy, and requires no maintenance as people fulfill changing roles within the company. However, it's a security risk because people can then perform tasks that they were not intended to perform or can access data that they were not intended to see.

Part of a company's cybersecurity approach includes limiting access based on each employee's job function. For example, Kevin is a human resources manager and Beth is a system developer. Kevin will need access to employee records and the Personally Identifiable Information (PII) that is associated with those records. Beth will need access to developer toolkits and source code. As a human resource manager, Kevin will never need access to developer toolkits and source code; likewise, Beth's role as a system developer will never require her to access human resource records.

DID YOU KNOW…

- ✓ Everyone in the organization doesn't need access to everything.
- ✓ Create defined roles based on job functions and assign access to systems and data based on the job the employee performs.
- ✓ Review access permissions on a regular basis.
- ✓ Insider threat is defined as someone within the organization that has access to systems and data that could harm the organization either intentionally or unintentionally. Limiting access through least privilege helps protect your company from this type of threat.

FACT 1: LIMITING EXPOSURE

Least privilege helps companies reduce insider threats, maintain confidentiality, and increase their overall security posture. Without least privilege, Beth would have access to human resource records and could view the sensitive records of every employee. If Beth had any bad intentions, she could use that information to steal other employee's identities. In turn, if Kevin has access to system development tools and source code, he could add a virus to the system or take the code to a competitor. Least privilege eliminates both of these situations by not giving employees access to systems and data that they don't need.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.