POLICE DIGITAL SECURITY CENTRE ADVICE GUIDE

Tips to Manage User Privileges

‘User Privileges’ is the term used for the level of access to online resources. Permission negligence threatens the integrity of business data and the security of the network. Strategic management is vital. Exercised well, strong controls will bolster the security of the business for very little cost. The following suggestions can reduce the likelihood of an incident caused accidentally or deliberately via excessive privilege, and prevent escalation of a breach:

Outline user behaviour in policies

Web browsing, social media usage and application download are prime opportunity for cyber attack. Block all activity that serves no purpose to business objectives, documenting the fact in policies issued to staff.

Restrict access to data

Losing control of data is not an option. Assign access according to job role, adopting a “least privilege” approach.

Restrict administration privileges

Designate admin level access to a minimal number of employees – DO NOT increase individuals’ access on a whim or for convenience. Administrators have all access privileges to system settings and controls, making them very attractive targets for the hacker and fraudster. Human error within an “admin account” is catastrophic because of the significant damage an attack can cause to the whole network. Provide a secondary or “user” account for standard business tasks – including web browsing and email to prevent accidental compromise of the network. The majority of the workforce does not require “admin rights”.

Limit Bring Your Own Device (BYOD) policy

Circumstance can require complete prohibition of BYOD on business premises. However, a controlled environment can balance employee happiness whilst maintaining security standards. Allow personal devices at specific times of day, in designated areas or restricted to a separate network.

Where possible, avoid using BYOD for business tasks or at least tasks involving company data. Ensure that employees cannot charge personal devices from the office desktops.

Segment the network

Prevent cross contamination and spread of malware by splitting and containing the network. External sources connect to the guest network, whilst business operates on the business network. Credentials to access the business network must remain confidential.

Restrict Removable Media

Rogue removable media can spread malware or steal information from the premises. Block USB ports if this privilege is not needed. Small and portable removable devices are easily lost or stolen. Only issue removable media when absolutely necessary.

Revoke privileges when employees leave

Disgruntled employees can become an insider threat once relieved of their duties. Removing user privileges of all “leavers” prevents data exposure, safekeeping sensitive business information. Don’t forget to deactivate email accounts that are no longer in use.

PDSC
POLICE DIGITAL SECURITY CENTRE