INTELECA

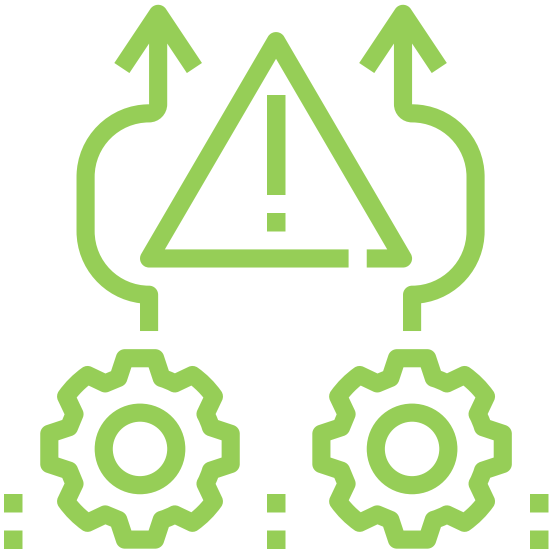
IT BUSINESS SOLUTIONS

Maintain the secure configuration of your systems and

SHORE UP YOUR SECURITY

Twenty-three percent—nearly one in four—IT security leaders cited system compromises as their biggest cyber concern and the greatest threat to their business (Neustar International Security Council [NISC]).

How do you fight off cyber crime and heighten the security of your systems? If you don't have policies and processes in place, and if you don't get rid of or disable unnecessary functionality, vulnerabilities will result and will compromise your system, leaving your organization defenseless against a cyber attack.



Risks to avoid

- ✓ Malicious hackers will exploit insecure system configurations by:
    - Exploiting redundant user rights or system privileges
    - Accessing data they are unauthorized to view
    - Building a back door for future use
    - Profiting from functionality that has been left in place and that has not been disabled
    - Connecting unauthorized equipment to either introduce malware or to compromise data
- ✓ System changes that are unauthorized leave your systems vulnerable and your data at high risk and open to serious security exploits.
- ✓ Exploitation of new software flaws occurs when systems are not patched as it provides hackers with unauthorized access to system resources and data. System vulnerabilities exist when patches have been issued, but not applied.

Measures to put in place

So, what measures can you put in place to shore up your systems and avoid exposing them to malicious attacks? Here are some security controls to implement that will help you avoid leaving your system vulnerable and open to malicious attacks.

Policies and Processes

✓ Update and Patch Systems

To ensure security patches are always up to date, develop and implement a comprehensive configuration and patch management process. Patching is critical for maintaining security as they are usually made available shortly after a vulnerability has been discovered. An automated patch management and software update process will also help to ensure they are applied and protecting your systems. If you can't patch a vulnerability, then you must take steps to make it difficult, if not impossible, to exploit.

In its 2018 Vulnerability Statistics Report, edgescan found that the lack of system patching is still a large source of vulnerabilities, and that configuration and maintenance are significant root causes of attacks ranging from Ransomware to data disclosure attacks.

✓ Create Configuration Control Policies

To ensure you securely control your system configuration, put in place security configuration management controls that will identify misconfigurations and any unusual changes to sensitive files or registry keys. This is critical as a few simple errors in system configuration could result in significant security vulnerabilities. With established processes, you reduce the likelihood of cyber criminals gaining access to your system and sensitive information.

Maintain the secure configuration of your systems and shore up your security

Inventories and Whitelisting

✓ Create Inventories

To identify unauthorized software or hardware, create inventories of all the authorized software and hardware in your organization. Include information such as location, owner, purpose, version, and patch status of all your software. An up-to-date inventory of your authorized software and hardware will help you to pick up any anomalies that might exist.

✓ Implement Execution Control and Whitelisting

Create a whitelist of authorized software you can execute: an approved software applications index that you permit to be available and active on your computer systems. Employ process execution controls to ensure your systems can stop the installation and execution of unauthorized software.

Implement Baselines, Scans and Supported Software

- ✓ Build a Baseline

  To effectively manage your operating systems and software, create a secure baseline to build on for all your components and systems. If you find that an application or a functionality doesn't support either a business requirement or a user, then remove or disable. You should manage the secure baseline build with configuration control practices, and if you find there are any deviations from your secure baseline model, then document and acquire approval.

- ✓ Conduct Consistent Scans

  For all your networked devices implement automated vulnerability scanning tools. Scans should be conducted regularly and any vulnerabilities managed and remedied immediately.

- ✓ Add only Supported Software

  Implement only those versions of applications, web browsers, and operating systems that are supported by a vendor.

Maintain the secure configuration of your systems and shore up your security

User Restrictions

- ✓ Restrict User Permissions

  Restrict users to only those permissions they require to do their job. These "normal" privileges will exclude installing or disabling any software or service.

- ✓ Constrain Internet and Email Access

  Those users with privileged system rights such as administrators should have their access to internet and email constrained; thus, avoiding a system vulnerability, limiting exposure to spear phishing, and reducing the ability of cyber criminals to achieve wide ranging system access.

- ✓ Disconnect irrelevant devices

  To add to the security of your systems, determine the need for access to removable media and peripheral devices. If ports and system functionality doesn't support the needs of the business, then disable them.

Research shows that a lack of basic security controls, such as those outlined above, can be the root cause of data breaches. So, implement these basic measures. Shore up your defenses, safeguard your system, and combat cybercrime. You'll stop system compromises from being your biggest cyber concern and the greatest threat to your business.

About Inteleca

As a global provider of IT Business Solutions, Inteleca has become a trusted partner in providing enterprise organizations with infrastructure and architecture design, hardware procurement, and maintenance services, excelling in the design of vendor-neutral solutions—as well as cutting-edge Optical Networking Solutions.