JAIGLO

Are you vulnerable to threats?

This quick security assessment will give you an overall idea of how well you're securing yourself or your IT environment.

Questions

Why we ask

1 Do you have a way to determine how many electronic devices and cloud services are in your environment?

◯ Yes ◯ No

Unaccounted for systems are a key vector for attackers. In 2017, manufacturing companies were hit hard by the WannaCry ransomware attack because many of them used unsupported legacy systems.

---

2 Do you have the tools to ensure an inventory of sensitive data?

◯ Yes ◯ No

Sensitive data is often stored in places no one intended, causing it to be forgotten and potentially made accessible to users without proper permissions.

---

3 Do you know who actually has accounts in your environment?

◯ Yes ◯ No

An often-overlooked aspect of security is that end-users may have too many account privileges, or may not be authorized to have accounts in the first place.

---

4 Do you automatically and regularly patch your systems?

◯ Yes ◯ No

60% of companies that have experienced security breaches say they could have occurred because a patch was not applied (Ponemon, 2019). Regular patching is necessary

Questions	Why we ask
5 Do you block unnecessary or harmful files from reaching you via email? ◯ Yes ◯ No	Email is the biggest vector for attacks. Despite transition to fileless attacks and phishing, attachments are nevertheless a common way to be breached.
6 Do you scan removable media or block auto-running of content in your environment? ◯ Yes ◯ No	In 2016, University of Illinois researchers left 300 unmarked usb flash drives around the campus, and nearly half of them were plugged into a computer within six minutes.
7 Do you keep track of how admin privileges are assigned among end-users? ◯ Yes ◯ No	The admin role has powerful permissions but its assignment is often unchecked, making it far too easy to miss hackers with illegitimate high-level access.
8 Do you look for patterns of malware events in your environment? ◯ Yes ◯ No	Malware events can occur as singular incidents, but hackers often launch large coordinated attacks with a barrage of malware.
9 Do you monitor login behaviors in your environment? ◯ Yes ◯ No	A popular way for hackers to breach systems is try logging directly into a targeted environment.

10 Do you regularly and automatically disable inactive accounts?

◯ Yes ◯ No

Half of all user accounts are dormant, and are favored targets for cyber criminals.

---

11 Do you regularly compare consecutive vulnerability scans?

◯ Yes ◯ No

Studying snapshots of vulnerabilities is a good short-term practice, but is insufficient long term.

---

12 Do you enforce policies for removing unauthorized hardware and software?

◯ Yes ◯ No

Unauthorized devices and software are easy paths for malware and other threats to enter your environment.

---

13 Do you automatically and regularly back up your most important systems and data?

◯ Yes ◯ No

Hard drives can fail, risking data breaches or permanent loss of critical information.

---

14 Do you have three copies of your data: two stored on different media, and at least one stored off-premises?

◯ Yes ◯ No

Backups kept in the same place as your original data are as at-risk as what you're trying to protect.

---

15 Are you able to restore critical systems after a breach or disaster within 90 minutes?

◯ Yes ◯ No

Restoring your data as quickly as possible can be the difference between your business closing its doors or keeping them open. The average cost of a data breach is $3.92 million (Ponemon, 2019).

Your results

Every “Yes” response is a reason to celebrate!
It’s the “No” responses, however, that you need to add up

5 or fewer “No“ responses

You’re doing well with regards to cyber security. You’ve put measures in place to improve your security posture. But this doesn’t mean your security journey is over! Have you looked into compliance requirements? How do you stay informed about emerging cyber security trends and threats? There are still conversations to have and actions to consider due to the constantly evolving nature of cyber threats.

6 to 10 “No“ responses

It looks like you can improve on cyber security measures you’ve already put in place. You’ve certainly raised your baseline security, but there’s more that can be done. Reduce your current risk even further by strengthening solutions and policies you’ve already implemented.

11 or more “No“ responses

It looks like you might be vulnerable. You could be breached by cyber criminals at any moment. There’s an urgent need to improve your security posture now, beginning with a detailed analysis of your network, endpoints and policies, followed by development and implementation of effective security solutions.

General recommendations

Below, you’ll find an overview of our recommendations for mitigating threats.

- Audit the devices in your network on a regular basis.
- Apply a data inventory and mapping solution.
- Create and regularly maintain an inventory of accounts in your system.
- Deploy a solution with automatic patch management to mitigate threats.
- Provide awareness training about the dangers posed by email.
- Provide awareness training for end-users and develop a policy to enforce that unverified media is not to be accessed on your network.
- Configure your system(s) to log changes in account activity, particularly for admin accounts and assigned privileges.
- Keep a log of malware events for your environment.
- Audit login activity in your environment to guard against suspicious activity such as logins from odd locations.
- Routinely review user accounts.
- Deploy a solution that automatically seeks out vulnerabilities, and study the evolution of vulnerabilities over time.
- Deploy a network scan or endpoint protection to defend against suspicious activity from devices connected to your network.
- Have a backup solution in place with options for automatic and regular data backups.
- Have three copies of your data: two stored on different media, and one copy stored very far away from your office(s).
- Have an enforceable plan in place to restore critical systems to the latest viable state as quickly as possible.