10 ways to prevent a DATA BREACH

A solid security posture is built by combining the right tools, techniques and expertise to shore up areas of exposure, and both federal and enterprise organizations must give security adequate consideration to avoid irreparable damages.

1 Employee training

Employee training should be your first line of defense against a data breach, period. **66%** of all malware is delivered through email attachments.* That's more than half! Phishing can't be done away with, but it can be combatted with employee training.

*according to Verizon's 2017 Data Breach Investigations Report.

2 Strong authentication

You need to ensure regular periodic password changes are taking place, and be sure to implement 2-factor authentication. This alone will get you more than halfway to protecting against breaches since **81%** of all incidents involved stolen or weak passwords.

3 Enforce the law of least privilege

The concept of "least privilege" is simply the policy of limiting an individual's access to data and devices that are not required to carry out their responsibilities. Most modern applications include role-based access from the get-go, but legacy applications may put the onus of security policy back onto you. When applied correctly, the law of least privilege can prevent a leak from becoming a flood.

4 Understand and reduce your footprint

It's not uncommon for an enterprise to have hundreds of devices that no one is using, which are sitting on the network, unsupported and unaccounted for. Trying to figure out what you have running and why is extremely important. From there, identify what you can remove, otherwise you're simply creating vectors for attack.

5 Patch and baseline management

Patch and update your apps and systems. Patching sounds like an obvious preventive measure, but patching at scale is a lot harder than it sounds. If you have 50,000 devices running a variety of different Operating Systems, with further varieties of versions and releases, all with different apps and patch versions for each, you've got a much larger job on your hands than you might think.

6 Supply chain and hardware/software custody control

As if you didn't have enough problems managing, patching and otherwise babysitting all the devices on your network, you also have to acknowledge that your devices could have been compromised before you took them out of the box. The best you can do in some cases is purchase only from reliable/reputable vendors, and stick to supply chains you have control over.

7 Trust management

Determine who and what you can trust. Who you can trust is pretty straightforward, and covered by the endless guides to mitigating insider threat, plus least privilege. What you can trust, however, presents a unique challenge at scale. Applications and frameworks that scale out to your entire infrastructure will likely require elevated or root privileges in order to function. This means that compromising one facet could lead to a compromise cascade, beginning with a single limited-privilege docker instance and ending with admin access to your entire domain.

8 Insider threats

Insider threats are a major issue when it comes to government security, whether you're talking about authority, responsibility, or access you trust any one individual with. Separation of duties is helpful, but overall it's a difficult problem to address and there's no single solution, which makes preemptive controls even more critical. When trust fails, you have to go to active defense: intrusion detection, firewalls, access control and VPNs are all ways to get proactive about protection.

9 Auditing

Periodic log review, review of access and review of accounts are key. Catch what you've missed and implement a robust, repeatable cycle of auditing, plus rinse and repeat when you fail. You will absolutely catch things you miss—everyone does. Log management is a great tool for helping you out with auditing.

10 Documentation

This often gets overlooked because no one wants to do it. If you don't, you'll eventually onboard a new person who won't have any clue what to do, how to do it or how things have been done. This is risky because in times of transition, no one is watching the gate, and new hires might not even know where the gate is, so to speak. Also included under documentation is change and configuration management!

August Schell specializes in partnering with enterprises and government organizations to comprehensively assess organizational security posture and build cyber security solutions that fit unique needs. Need help operationalizing some of the tactics above? Reach out to an August Schell specialist now.

www.augustschell.com | inforequest@augustschell.com | 301.838.9470

augustschell