YOUR ACTION PLAN FOR ADDRESSING RANSOMWARE

In 2017, ransomware – the use of weaponized encryption to block access to a computer system or service until a ransom is paid – is all the rage among hackers.

Ransomware is now one of the top three most common malware threats.

The situation is dire, with hackers requesting ransoms of up to **$73,000** per attack.

Ransomware payments totaled more than **$1 billion** in **2016**.

A massive jump from the mere **$34 million** paid in **2015**.

The costs of ransomware attacks aren't limited to a bitcoin payoff. In manycases, the additional costs can dwarf the initial ransom like:

Disinfecting machines

Stabilizing systems

Restoring data

To make matters worse, it could be days or even weeks after an attack before your network is fully operational. Prevention and preparation for ransomware attacks are a worthwhile investment.

WHAT'S THE BEST WAY TO MAKE SURE YOUR ORGANIZATION IS PREPARED TO FEND OFF RANSOMWARE STICK-UPS?

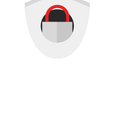
1 HAVE A PLAN

It's important to have a plan in place detailing the actions your organization will take in the event of a ransomware attack.

2 BACK UP YOUR DATA

Your data should be backed up on a daily basis. **The 3-2-1 principle** is a good rule of thumb here:

- Keep at least three copies of your data
- Back up your data on at least two different storage types
- Keep at least one backup copy off site



3 EDUCATE YOUR USERS

Phishing emails are the most common method of ransomware distribution.

It's important to tech your users how to identify suspicious emails and links.

4 MAINTAIN STRONG PERIMETER DEFENSES

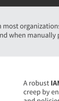
Anti-malware and antivirus are your first line of defense against ransomware.

Good ones will be able to detect and stop many ransomware variants.

5 BLOCK ADS

"Malvertisements" are a standard method of distributing ransomware.

You can lower your risk of infection by using ad blockers to keep ads from being served to your users.



6 PATCH, PATCH, PATCH

Out-of-date applications and operating systems are a favorite target of ransomware attacks, so keep your apps up to date.

Don't overlook the importance of **Stronger Identity** and **Access Controls**

You can't ignore the role that modern **identity and access management (IAM)**tools play in preventing and minimizing the success of ransomware attacks.

The principle of least privilege says to limit access to applications and data to those who need it, when they need it.

In most organizations, users have more access than they should, especially IT administrators. And when manually provisioning access, errors are bound to happen.

A robust **IAM** solution will prevent this kind of access creep by ensuring the consistent application of rules and policies across your organization.

Strong **privileged access management (PAM)** capabilities, such as time- and location-based access controls, will help:

Implement least privilege

Minimize your ransomware attack surface

Strengthen your security with **Enterprise-Grade Multi-Factor Authentication**

One of the easiest ways for hackers to gain access to your systems is by hijacking static passwords, which:

Can easily be cracked

Can often be purchased in bulk for pennies on the dark web

Passwords are clearly inadequate, but the issue can be resolved by implementing **multi-factor authentication (MFA)** across:

1. Your privileged users
2. Applications
3. Your servers
4. Your business-critical network systems
5. Virtual private networks

By using push notifications and smartphones that your users already have, **MFA** can be a simple and increasingly inexpensive way to block ransomware attacks, even in the event that credentials are compromised.

In the end, **there's no silver bullet** for stopping ransomware attacks.

But by following the best practices above and implementing some advanced **IAM** solutions, you can put your organization in a much less vulnerable position.

It's your decision: **Invest in security today or invest in bitcoins tomorrow.**

+1 (877) 221-8401
sales@identityautomation.com
identityautomation.com
7102 N Sam Houston Pkwy W, Ste 300
Houston, TX 77064

IDENTITY AUTOMATION™