Top Ten Actions during a Ransomware Attack

When you're under attack, you're under pressure. You can't risk losing sensitive data, damaging customer loyalty, or disrupting the business. Now is the time to put procedures in place that will work during high-pressure circumstances like a ransomware attack. Make sure staff knows what to do and how to do it by focusing on these critical steps.

1

Contain the attack.

At the first sign of a breach, isolate impacted systems on the network by disconnecting them completely or quarantining them in a private network enclave. This will help stop the spread and minimize damage.

2

Lock down your environment.

Never fully shut down systems or turn off the power! That will reduce or eliminate the ability to forensically analyze those devices later. Update credentials and passwords on clean machines. If any information was posted on your site by the attackers, remove it and contact search engines to clear the cache.

3

Execute your backup communications plan.

If your systems are down, it's time to use your well-defined communications plan. Inform leaders and internal stakeholders about the attack, whether it's via mobile phone or an alternate email address. Alert IT and security teams, senior leaders, and outside security consultants ASAP.

4

Mobilize your emergency response team.

Your breach response team should have been assembled with some key players, such as forensics experts, legal, InfoSec, IT, investor relations, and corporate communications. Everyone on the team needs clear instructions, as should others involved in recovery. Read this "Hacker's Guide to Ransomware Mitigation and Recovery" ebook now, before you need it.

5

Launch your external communications plan.

Contact critical partners and authorities. Engage external tech partners to help, including your storage provider. If you work with the media, regulators, and legal teams after an attack, maintain an updated list of law enforcement contacts, such as the FBI in the United States. Contact your cyber insurance providers and mention any compliance obligations and potential penalties.

6 Notify affected customers and businesses.

Notify affected customers and businesses. You might have drafted a notice and letter to help you properly relay the information you're obligated to share, recommendations for those affected, and a clear statement of what you plan to do next.

7 Begin the forensic process.

With proper network monitoring tools in place, security and access logs can help you identify the source of an attack fast. These logs can also provide the required proof of compliance to regulatory agencies. Make sure they're adequately protected and secure from deletion.

8 Triage impacted devices.

Triage any impacted devices and prioritize them for forensic review. Your security team determines what type of attack was launched and how broadly it's impacting your environment. The faster this happens, the faster your team can apply patches and restore a clean backup. Once that's done, begin the restoration process into a staged environment. Prepare your environment for any investigation down the line, with a well-defined handoff process.

9 Move to a clean recovery environment.

It's time to begin your actual physical recovery. Your recovery environment should be staged, tested, and ready to do. This gives you a prebuilt way to get back online right after an event, including a line of sight to new hardware and systems. You might not be able to use your existing hardware, which could be taken by authorities or investigators as evidence or for quarantine.

10 Get back on track.

Having clean hardware, like the clean storage environment shipped to you next business day with Pure Storage® platform Cyber Recovery and Resilience SLA in Evergreen//One™, can get you quickly back on track. It's not just a temporary fix. We'll provide you with a full recovery plan, a data transfer rate, and bundled professional services to assist with migration to your clean arrays.

Be Ready for Recovery with Pure Storage

Knowing the immediate steps you can take during the early stages of an attack can help minimize loss, cost, and risk. Pure Storage can help you take swift action during an attack by:

- Providing always-on data-at-rest encryption, with no performance overhead or management required
- Eliminating the ability for protected data to be modified or deleted, thus ensuring recoverability

PS2665-01-en 09/24