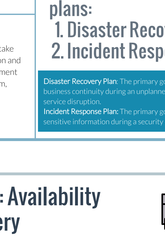
How a Back-up Strategy can save your Business from Ransomware

Information and information technology are inextricably linked. However, most of the time the focus is on technical security measures and the technical side of an attack. The value and importance of the information itself tends to take a backseat.

The Security Service of Aruba (SSA) strongly believes that you need to understand the value of your information/data in order to better protect it. A risk-based approach helps you identify how valuable your data is and as such helps you choose the right strategy to better protect them. Below we highlight only the main aspects for employing a data backup and recovery plan.

01 Identifying & Managing Risks

For information to be managed it must be clearly identified. Know the value of your information in order to assess the risks if they are stolen, corrupted or made inaccessible.



Plan Ahead: Create a Recovery Plan 02

Once you identify your critical data, applications, and processes you can define how you will recover.

Your recovery response should take many variables into consideration and should clearly identify and document what is to be recovered, by whom, when, and where in a detailed recovery plan.

In general there are 2 types of recovery plans:

1. Disaster Recovery
2. Incident Response

Disaster Recovery Plan: The primary goal is to ensure business continuity during an unplanned outage or service disruption.
Incident Response Plan: The primary goal is to protect sensitive information during a security breach.

03 Backups: Availability & Recovery

Data can be backed up in different ways

FULL	DIFFERENTIAL	INCREMENTAL
You may want to do a full backup periodically (weekly or monthly) and before any major system upgrades.	A differential backup only creates a copy of data that has changed since your last full backup.	With incremental backups, you're only storing the data that has changed since your last full or differential backup. Each increment is saved as an incremental volume

Backups: 3 Options for Storing 03+

ONSITE STORAGE

Your backups are stored within the physical space of your organization. It's convenient and readily available should you need to start your recovery process. If this is your only storage you may still experience data loss if you are affected by fire, flood or ransomware - for example.

OFFSITE STORAGE

Storing backups of critical data in a separate, offsite facility can help your organization prevent data loss.
If you plan to contract a vendor for offsite storage, make sure that they have security measures, incident management processes, and a disaster recovery plan in place.

CLOUD STORAGE

Cloud-based storage can be beneficial in many ways. It frees up space, you can benefit from the expertise of the cloud service provider. However, you should ensure that the service provider you select can support your security requirements with proper safeguards. Also consider data residency - know where your data is stored geographically.

Online or Offline Backups?

Online

Online backups are stored on a remote server or computer that is connected to your network. They are likely to be affected by many cyber threats such as ransomware, thus compromising your backups.

OR

Offline

Offline backups remain unconnected to your organization's systems and are only connected when they are required. Because these offline backups are not connected, they remain unaffected by many cyber threats, like ransomware, that can compromise all systems and devices on your network.

Follow the 3-2-1 Rule

The 3-2-1 rule can help in designing your backup process. This rule means that you have 3 copies of your data on 2 different media (e.g. different physical hard drives) with 1 copy at a different location for disaster recovery (e.g. physical).

Remember to restrict access to your backups!

Consider encrypting your backups

There are many reasons why having a backup plan will benefit you in the long term such as:

RANSOMWARE
A type of malicious software that locks you out of your system. You won't have to pay the ransom if you have backups

FAILURE OR OUTAGE
Backups can ensure that your organization doesn't lose critical information due to a failure, crash or unplanned outage

DENIAL OF SERVICE
Threat actors use these attacks to disrupt services and or cause a distraction to steal data. With backups & a recovery plan you can minimize downtime during recovery

NATURAL DISASTER
Natural disasters can cause damage to buildings and physical assets that may restrict your ability to access them. Backups in a secondary location can help.

CYBERSECURITY AWARENESS MONTH

REFERENCES

- Risk Management: The Value of Information as Point of Departure - National Cyber Security Centre Netherlands - July 2020 - www.ncsc.nl
- Guide to Cyber Security Measures: Step by Step to a Digitally Secure Organisation - National Cyber Security Centre Netherlands - June 2021 - www.ncsc.nl
- Developing Your IT Recovery Plan (ITSAP.40.004) - Canadian Centre for Cyber Security - January 2021 - https://cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004
- Tips for Backing up Your Information (ITSAP.40.002) - Canadian Centre for Cyber Security - October 2020 - https://cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002
- How to Prevent and Recover from Ransomware (ITSAP.00.099) - Canadian Centre for Cyber Security - September 2021 - https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099
- Internet Organized Crime Threat Assessment 2020 - EUROPOL - www.europol.europa.eu
- Keeping an Eye On Information Security: ISO Standards ISO/IEC 27001, ISO/IEC 27014 - https://www.iso.org/news/ref2604.html
- Ransomware - FBI - https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- Ransomware: What It Is & What To Do About It - National Cyber Investigative Joint Task Force https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf
- Ransomware: What board members should know and what they should be asking their technical experts - National Cyber Security Centre UK - 2 June 2021 - https://www.ncsc.gov.uk/blog-post/what-board-members-should-know-about-ransomware
- Create your Cyber Action Plan - National Cyber Security Centre UK - https://www.ncsc.gov.uk/cyberaware/actionplan