Top 7 Document Automation Vulnerabilities and How to Prevent Them

Windward Studios White Paper

windward studios

Contents

Although document automation software provides better security for your documents than the old way of managing them in a filing cabinet, there are still loopholes that can create vulnerability. Being alert to the possible threats makes it possible to secure those documents.

When is Document Automation Most Vulnerable?

There are four crucial vulnerable instances that organizations need to be cautious about. At these points, the threat can come from within or outside.

Document automation vulnerabilities manifest at these points:

- **When you are entering data into the document**
- **When you are transferring or sharing documents**
- **While document is simply being stored**
- **As you access the document**

The following are the seven common document vulnerabilities that have been identified by industry experts. Luckily though, there are also remedies to these threats:

MAN IN THE MIDDLE ATTACK
CLOUD STORAGE
DEVICE THEFT
EMAILING INFO
EXTERNAL DATA
HARD COPY DOCS
HUMAN ERROR

Man in the Middle Attack

This is an attack that exploits the different weak spots that make up the 7 vulnerabilities above. With the man in the middle attack, a hacker will position themselves between the user and the next endpoint. This could be between a user and an email correspondent, a cloud server, or even a browser.

The man in the middle intends to steal vital information such as

- Login information
- Account data
- Personal information
- Private communication

The purpose of this may vary and depend on the organization that the man in the middle is targeting. Financial institutions may be targeted in order to commit fraud, medical records may provide information that can be exposed for some kind of gain and at times it is to discredit the organization whose documents has been stolen.

Certain points of the document automation system can be more vulnerable to this kind of attack because they do not have encryption. The methods the attacker will use include:

- Inserting spyware that records data in the documents
- Session hijacking using public Wi-Fi connections
- Hijacking email communication
- HTTP interception

How to Prevent a Man in the Middle Attack

Although the man in the middle attack can result in a major embarrassment to an organization just like the Wikileaks scandal, it is possible to prevent them with simple strategies. The hackers may come up with new ways to intercept, but they can always be discovered and plugged up. Here are the main ways to prevent these attacks:

- Invest in software that can identify, intercept, and eliminate any spyware within the system.
- Ensure that employees does not use public and unfamiliar Wi-Fi connections to access the server or share vital documents via email.
- Use secure SSL to send all information via end to end encryption.
- Ensure that only authenticated devices can access documents shared within the network.

Cloud Storage Vulnerability

Most document automation systems will make use of cloud storage. It is an efficient way to store documents in a place that can be accessed with ease and the business does not have to worry about maintaining servers.

However, cloud storage is an offsite storage system and that makes it vulnerable to infiltration. It is also a shared storage system that can be accessed from different points. According to NSA, most vulnerabilities with cloud storage are self-inflicted. The users of these systems may open themselves up to threats in the way they set up the system or the way they use it. The common loopholes in cloud storage include:

- Misconfiguration of the system due to poor understanding of shared cloud systems
- Weak access control methods causing a breach in authentication procedures
- Use of single-factor authentication
- Hackers with knowledge about system weaknesses that they can exploit

Preventing Cloud Storage Vulnerability

Since most times the weaknesses are a result of the way the system is used, it is easy to fix any vulnerabilities. The recommended fixes include:

- Utilize third-party tools that can identify misconfigured cloud policies
- Ensure all staff are well trained about the working of the system and how they can prevent vulnerabilities
- Use multi-factor authentication (MFA) as well as regular reauthentication
- Run regular audits to identify documents that may run the risk of being exposed
- Protect API keys by excluding them from software version control systems that may cause leaks
- Always have documents encrypted with 256-bit encryption when stored as well as when in transit
- Regularly change authentication passwords

Device Theft

The beauty of document authentication is that it allows access to documents using any device that has a connection to the internet. This means employees can access them from any location using their personal devices like mobile phones, laptops, and so on.

Unfortunately, this is also a vulnerability. There is no guarantee that these devices will only be in the possession of their owners. When these devices are stolen, it may be very easy for intruders to gain access to email communication, passwords as well as clear access to information. While in possession of the stolen device, the thief can assume the privileges of the owner and access all the information their level of clearance allows them to have.

There is also the fact that most people will store passwords on their browsers for easy access which means possession of these devices is a wide-open door for access to every information that should be secured.

Preventing Vulnerability Caused by Device Theft

It would be much easier to prevent the theft of these devices in the first place. You can find out different ways to keep your devices safe like not leaving them unattended in public places, not carrying an obvious laptop bag, and not carrying them in places known to be unsafe. That though is no guarantee that they will not be stolen so you can also do the following:

- Fully encrypt every sensitive information on your personal devices
- Use multi-factor authentication like biometrics and password access
- Install security apps like Prey which you can use to wipe all information from your device once it is stolen
- Inform technical support the moment your device is stolen so that accessibility is blocked
- Reset your email passwords immediately

Emailing Information Vulnerability

Document automation usually includes emailing documents to clients, team members, and other concerned individuals. This process of sharing information might be one of the most vulnerable situations. For example, if a bank emails account details to a client, there is no way of knowing whether the recipient may have left their computer unattended to and someone else saw the message and copied those details.

Email can serve as an entry point for attacks as well as a leak for documents. Here are some of the vulnerabilities created by email:

- Unencrypted information can easily be accessed by third parties.
- Hackers can send malware and viruses through email and they will infect the entire system.
- Opening emails using administrator privileges can open the system to unauthorized access
- Emails can be intercepted by a man in the middle attackers.
- Sensitive information may be exposed if someone forgets to log out of their email account when using a shared computer.
- If a device is stolen, emails are one of the first things that thieves will harvest for data and documents.

How to Prevent Email Vulnerability

- Confidential documents should always be sent using encryption so that it is downloaded directly from the server using authentication keys.
- Have a reliable antivirus and do not open attachments from unfamiliar sources.
- Be careful about clicking the unsubscribe button on unsolicited mail, hackers also use that to introduce malware into your system.
- Do not open emails using administrator privilege
- Activate automatic logout for emails if they are left open on public computers for a particular duration.
- Always logout from your email and never open it on a public computer.
- Use secure passwords and change them regularly so that if the device is stolen, it is hard for the thief to gain access.

External Data Sources

Document automation may depend on external sources to provide updated data. For example, as an organization prepares a presentation, they may use the internet to find updated figures about particular reports. Since these are sourced automatically, it is possible that hackers can use this as a way of gaining information from your server. Trojan horses for example may disguise themselves as packet data with the kind of information you are looking for and once accepted into the system, they will begin to send information back to the hacker.

It is also possible for people within the organization to enter the wrong data into the system and this might be used in all documents, affecting the credibility of an organization.

How to Fix External Source Vulnerability

- Invest in software like firewalls and antivirus that can identify external threats that may be trying to gain access to the system.
- Verify the sources that you use to access data for document generation
- Limit who can add or edit data on the server

The Existence of Hard Copy Documents

While automation will make most documents paperless, there may still be some hard copy paper documents that are printed, scanned, or even faxed. These present a serious problem especially for medical organizations that are supposed to adhere to HIPAA regulations.

It is much harder to ensure privacy and confidentiality with paper documents. Imagine a scenario where a document is printed but the person who prints it forgets to retrieve it from the shared printer, that information can end up in the hands of anyone and compromise the rest of the stored information in the server.

Also, in the process of scanning hard copy documents, this information is vulnerable to hacking and man in the middle attacks since it is not encrypted at that point. This can compromise privacy as well.

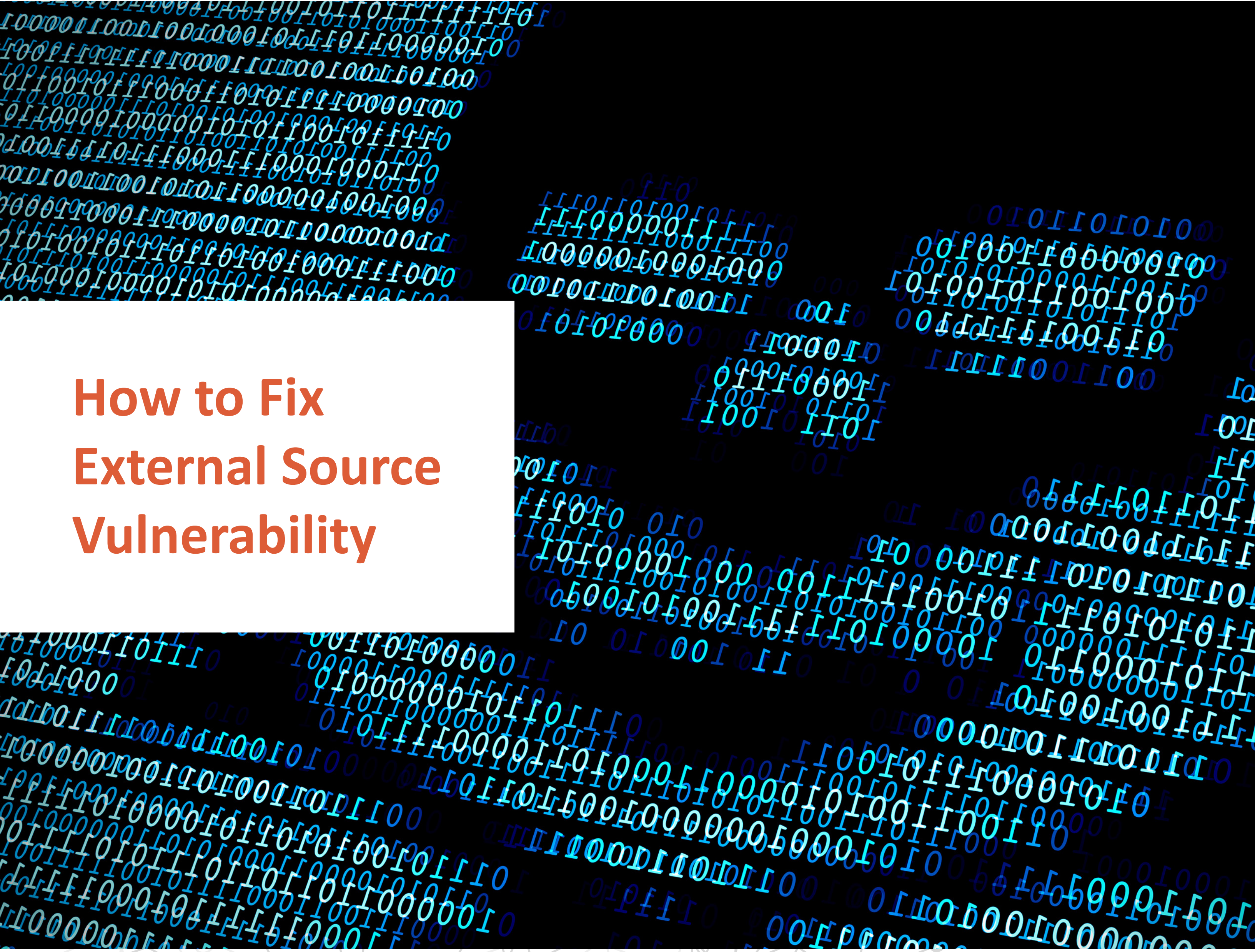
Preventing Vulnerability Caused by Hard Copy Documents

- Printers can be upgraded to print only with physical authentication access, which means the documents will only be released by the printer when the person who printed is physically at the printer and presents authentication.
- Scanned Documents need to be encrypted once they have been scanned so that they have an end to end encryption.
- Invest in software that will eliminate the presence of hard copy documents.

Human Error

Although, for the most part, the process of automating documents is free from human involvement, it cannot entirely be automated. When humans get involved in some processes, they can make the process vulnerable. There are many cases in which human error can create vulnerabilities. These include:

- Entering the wrong recipient and sharing private documents with them.
- Forgetting to log off when using a public computer.
- Writing down passwords and living the paper exposed.
- Using weak passwords that can easily be guessed or hacked like names of your children.
- Emailing authentication information without encryption.



How to Fix External Source Vulnerability

- Make sure everyone knows how to use the software to avoid making errors that will expose the entire system.
- Use auto-logout so that access is safeguarded even if someone forgets to log out.
- Encrypt all sensitive information so that only specified end users can access documents with authorized authentication.
- Use software that can retrieve information sent to the wrong person.
- Encourage the use of password management software to avoid writing down passwords.
- Guide people to be more responsible.

In Conclusion

Vulnerability is not static. It is necessary to periodically carry out vulnerability audits to see if there may be a loophole created either because of new processes introduced or even newly authorized individuals. It is also essential to encourage everyone that uses the document automation software to vigilantly prevent any threats.

In the end, automation improves the security of documents and ensures that information is trusted. By addressing the vulnerabilities, the document automation process can get closer to perfection.