WHITE PAPER

Cybersecurity for Salesforce

Virus Scanning:
Solving the Weak Link

Table of Contents

Introduction

Salesforce® is the most widely used customer relationship management (CRM) application in the world. It boasts millions of users and offers a truly integrated platform with a global "community" to address a wide range of business areas within the sales, marketing, and customer communications. However, the platform does NOT provide a way to prevent users from uploading certain types of files or scan attachments, document uploads, or chatter for viruses or malicious content.

For Salesforce, this is an intentional decision since none of the virus code gets executed on their systems as it is never executed, just stored in their database. This is where they rely on their partners to help fill the gaps in the product. Scanning viruses is not their core competency, and why they have chosen not to implement a native solution. The same goes for box.com and other applications.

As a result, there is a huge security risk for all Salesforce users, especially when a Salesforce application is publicly exposed through communities and sites.com. The last thing any company needs is a harmful file uploaded in Salesforce, infecting their network and corrupting or exporting your sensitive data. Thankfully, there is a partner solution that has been developed by certified Salesforce architects to mitigate the risk – EZProtect® Anti-Virus Scanner.

Areas of Vulnerability

There are generally three areas within a Salesforce environment where users would attach a possibly infected file:

1. Documents, attachments, and content
2. Chatter
3. Community Portals

Documents, attachments, content, and chatter are typically used by internal employees. Community portals may be used to support internal employees, but public-facing portals where files are uploaded by the public directly to Salesforce pose an additional threat and major vulnerability. There is no way to ensure that files/attachments have been scanned for viruses before being submitted as files are coming in from the public, so a third-party virus scanning tool is necessary to protect the Salesforce environment.

Although corporations and government entities do have virus scanners on desktop and laptops, it doesn't mean they are completely protected. There are countless cases, especially with laptops, where the virus scanner is outdated because something happened to the machine where the automatic updates didn't go through. This is one of the biggest misconceptions IT security and business professionals have which poses the largest threat to organizations.

Essentially, Salesforce administrators and security specialists need to consider how the Salesforce environments are set up for both internal and external threats as there are several ways in which a corrupt attachment can make its way into a Salesforce environment – chatter, the documents/attachments/content areas, and community portals.

Anywhere there is an opportunity to attach a file and submit to the environment, there is a direct risk to the company. If an infected file is submitted via chatter, online form through a portal, or just attached as a supporting sales document, all it takes is for a reader to open the file and the entire Salesforce environment will be infected. It's that simple.

Current Threat Vectors

Any file that is uploaded to Salesforce brings with it the opportunity to carry a virus, malware, or unintended active content. There are four main avenues for these types of files:

1. Attachments (cases, leads, opportunities, etc.)
2. Documents
3. Content Files (including Chatter)
4. Static Resources

Each of these areas offers its own opportunity for virus/malware infection.

Standard Threat Scenarios

There are four standard scenarios which should be addressed within any Salesforce organization.

A. Files that are uploaded by customers or partners and opened by customers or partners

B. Files that are uploaded by employees and opened by customers or partners

C. Files that are uploaded by customers or partners, and opened by employees

D. Files uploaded by anyone which contains a virus that is not yet recognized by scanners but is eventually.

Scenario A is probably the most severe threat. You don't know if the customer or partner has a virus scanning capability on their documents — either on the sending or the receiving side. You don't know if they are malicious actors trying to intentionally harm other customers or your company. You also probably want to show your own lawyers and compliance officers that you are making a best effort to protect your customers and partners.

Scenarios that deal with employees can be dangerous as well. Many companies do have policies and practices to include virus scanning software on all of their internal computers. However, this software may not be up-to-date as they are often installed on each, individual system, and current viruses will be missed. And employees increasingly bring-their-own-devices into their work, including tablets, phones and personal computers which may not include virus protection. Many company environments do not lock these devices out.

In Scenario D, at the time of initial upload, a file is scanned by a virus protection software and marked as clean as the virus was missed or not yet recognized. So, although the virus scanner marked it as clean, the file actually contained updated malicious content that the virus scanner missed. This scenario is actually quite a large threat as all virus scanners are only as good as the currently known dictionary of viruses, and hackers are constantly coming up with new pieces of malicious code.

The Solution

Designed for large enterprises, EZProtect easily scans chatter files, documents, attachments, and content for harmful viruses. Through careful and clean design, EZProtect makes the detection and deletion of viruses, malware, Trojan horses and other malicious threats effortless and painless. Key features include:

- File-type scanning allowing users to specify a list of file types that are allowed or denied (whitelist or blacklist
- Scanning of PDF files that contain JavaScript and therefore may contain malicious code
- Scanning of static resources as well as document, attachment and content versions
- Skip scanning one or more of the file objects – attachments, documents, content versions and static resources.

By default, EZProtect scans for viruses, malware, and Trojan horses with an add-on capability to scan for JavaScript content in PDFs (JavaScript is executed when PDFs are opened in the browser). It also offers the additional ability to re-scan existing files already present in the system to look for viruses and other threats that have been identified since the file was initially uploaded.

Standard Objections

1. Scanning via Email – "Why do we need EZProtect when we already have a virus scanner for our email systems? All files we upload to Salesforce would have already been scanned."

Example: Someone could easily receive an email in their email inbox (via Microsoft Outlook) that was not flagged as junk for some reason. The email, which contains a word document attachment includes a Macro with a malicious script. The document is then downloaded out of email and into Salesforce containing a malicious script and released within the network.

Answer: Scanning within email is not full proof as many viruses are missed and things can still get through. EZProtect itself is not foolproof either, but the more applications you have in place to prevent malware and viruses, the more protected a company will be.

2. Triggers within Salesforce – "All you have to do is create a trigger on an Attachment object."[iv]

Example: Your Salesforce administrator can write a Trigger on an Attachment Object to detect viruses within the attachment.

Answer: There are essentially two things going on here. The first part is, you need to know when files are being uploaded. The second part is detecting the viruses, malware, pdfs containing Javascript, and files of certain types. The trigger part only handles the detection that a file is being uploaded — that's part one. Part two is the more difficult part and there are several variables. So, this is not a comprehensive solution and will not address the other two areas where viruses may

be lurking – documents and static resources. In addition, triggers often fail or turn off without notification when they hit certain volume thresholds.

Conclusion

Cyberwarfare is an ongoing threat that will only continue to gain more and more traction. As enterprise-level businesses continue to lock down their resources and spend more and more money on education and infrastructure, cyber-attacks could very likely begin targeting smaller and smaller businesses, in order to gain access to their target.

In other words, no business is immune. No matter the size of the company, sector, demographic served, or type of data housed. This is especially true when companies are doing business overseas. Those employees could serve as easy marks to bring malicious code to systems, unbeknownst to anyone.

The first computer security hack occurred in 1903 when magician and inventor Nevil Maskelyne disrupted British engineer John Ambrose Fleming's demonstration of what was supposed to be a secure wireless telegraphy device. The hack sent insulting Morse code messages to the auditorium's projector. Needless to say, attacks have been on the rise ever since.[i]

According to Symantec, half a billion personal records were stolen or lost due to nine megabreaches in 2015. The number of exposed identities jumped to 429 million. That data comes only from the information reported.[ii] Even with security technology constantly improving, businesses are more vulnerable than ever. As the hackers continue to breach the barriers of security, it is on the shoulders of businesses to do everything they can to prevent attacks. But are we doing everything possible?

In May 2016, Tech Pro Research conducted an online survey focused on cybersecurity to find out what's being done to prevent attacks and how businesses react in the event of such an attack.

Key Findings

- Forty-five percent of respondents said mobile devices pose the biggest security threat to their business.
- When it comes to strengthening their weakest security links, respondents believe educating end users and management is often the best solution.
- Of respondents whose companies do business overseas, 76% feel this presents an added challenge to security.
- The majority (60%) of respondents said their companies do not use digital forensics.
- Among respondents whose companies do use digital forensics, 42% said it has uncovered an issue in the past year.
- Forty percent of respondents said their business has not been the target of a cyber attack.

- Of those that have been attacked, roughly half are working with a government agency on the issue.
- Sixty-five percent of respondents are highly or moderately concerned about cyber warfare attacks versus run-of-the-mill attacks.[iii]

The best way to prevent an attack within Salesforce is to install a third party virus scanner like EZProtect, but also, strengthen policies on education within your organization.

- IT staff and end users must be informed, not only on the ins and outs of how systems work but how easy it is for outside forces to influence and break down company security. IT staff should help end users understand the security threats within Salesforce so they won't accidentally hand over the keys to the kingdom.
- Leaders should educate IT staff and users on the dangers of loading unsecured documents into Salesforce and educate them on the four security holes that exist in the system.
- Finally, leaders should ensure everyone has read and agrees to a company policy that is frequently updated to reflect the ever-growing shift in a very challenging landscape.

EZProtect is the only solution designed by certified Salesforce architects who understand the vulnerabilities of Salesforce and supports scanning of multiple Salesforce environments under one license, on both commercial and FedRAMP approved hosting. The company, Adaptus, is also domestically based which is important to both state and federal government agencies and employs active development on the product to expand to other cloud-based tools such as box.com and others in 2018. For more information visit www.adaptus.com/ezprotect

About Adaptus

Adaptus, LLC is an application development and Salesforce architecture consulting firm based in Austin, TX. Founded in 2012 on the premises of collaborating with customers to solve real problems, Adaptus products are used by large, Fortune-500 companies with thousands of users. Adaptus provides reliable, high-quality and cost effective information technology solutions and custom cloud-based computing applications designed to integrate with Salesforce.com. Our applications and architectural consulting services help businesses optimize their operations by working smarter, while increasing productivity and profitability. Led by certified Salesforce architects, Adaptus specializes in customer-driven product solutions to provide highly relevant, efficient and cost-effective solutions for large-enterprise users around the globe. For more information about our products, or to request consulting services, please visit www.adaptus.com.

End Notes

[i] Cybersecurity Research: Weak Links, Digital Forensics, and International Concerns, Tech Pro Research, September 2016
[ii] Cybersecurity Research: Weak Links, Digital Forensics, and International Concerns, Tech Pro Research, September 2016
[iii] Cybersecurity Research: Weak Links, Digital Forensics, and International Concerns, Tech Pro Research, September 2016
[iv] http://explore.wave6.com/blog/salesforce-upload-attachments-blocking-potentially-harmful-files