DigitSec, Inc.

Ignorance is Not Bliss

What happens when Salesforce software is misconfigured.

Salesforce 'out-of-the-box,' is a secure platform which can be trusted to store data in the cloud. However, once a company starts customizing their Salesforce and adding custom code or third-party extensions, they open themselves up to attack. This is because Salesforce's security promise only covers the variables they can control. Software misconfigured by outside, uninformed developers and/or administrators is the customer's responsibility.

In many cases, companies do not realize their joint security responsibility with Salesforce until it's too late. Take the Internet Corporation for Assigned Names and Numbers (ICANN) for example. This large, non-profit organization utilizes Salesforce to help them ensure the Internet's network is stable and secure for people using it around the world. In other words, ICANN relies on Salesforce to help it maintain the backbone of the Internet. On April 30, 2015, ICANN regretfully announced its Salesforce data had been exposed 330 times over the span of 11 months.

ICANN's data not secured
for 11 monthes

ICANN's security experts - didn't detect the breach

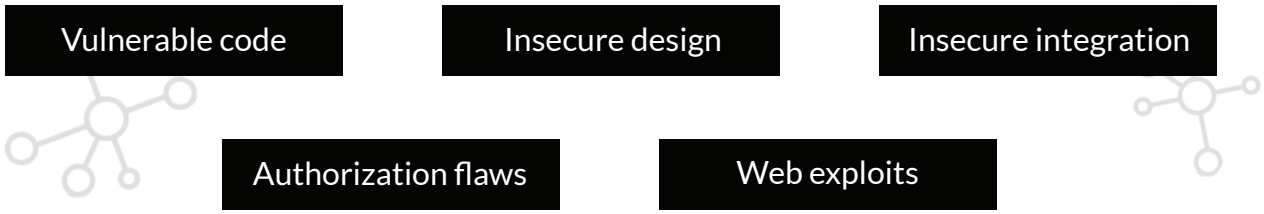
ICANN's Salesforce admins - didn't detect the breach

ICANN's developers - didn't detect the breach

Why ICANN was vulnerable to attack

ICANN's Salesforce environment which was storing customer data, was misconfigured. Since the data breaches occurring were not instantly obvious to ICANN's security team, their data continued to be repeatedly exposed for nearly a year. While ICANN's data breaches stemmed from a security issues with their Salesforce's advanced search feature, there are endless other potential openings for any company where data can be exposed.

Common ways Salesforce software becomes misconfigured and susceptible to hackers:



This establishes the following facts:

- Companies using the Salesforce Cloud do not always pay close attention to security and can be operating under dangerous assumptions.
- There are many ways a Salesforce deployment can be attacked which customers are unaware of.

How Salesforce organizations can protect their data

The easiest and most effective way for a Salesforce organization to protect their data is to enlist the help of DigitSec, Inc.'s security tool, S4 - SaaS Security Scanner for Salesforce (S4). S4 rapidly identifies vulnerabilities in APEX code developed using the Force.com development environment. It is a cloud based application and utilizes a combination of static code analysis and runtime testing to help companies protect themselves against data breaches and hackers.

With one click, S4 can run a comprehensive security scan against any-sized code base in Salesforce. It then enables companies to pull up an application security report with detailed findings. Each finding is prioritized based on the level of risk and potential impact to the company's data, and is accompanied by clear guidance on how to remediate the threat and secure the Salesforce instance.

Had ICANN secured their Salesforce instance with S4, their data would have been safe.