BIZCOMMUNITY

Does your startup take data privacy and security seriously?

By Charles Mburugu

21 Oct 2015

You must have read that the number of online attacks and computer system hacks are rising each year. Just a week ago, the Office of Personnel Management in USA has reported that more than 21 million people have been affected by a data breach stealing fingerprints, social security numbers and other personal information from US government computer systems. And you must have heard about the iCloud breach last year, where hackers stole private photos from thousands of iCloud users, many of them being celebrity A-listers.

No matter what we do, we cannot totally eradicate these types of security threats. The best that a company could do is to stay prepared and adopt all sorts of security measures to minimise the vulnerabilities within the system. We have listed out some core issues for you to immediately look into, and adopt a safer practice wherever possible.

1. Choose a dedicated server over shared ones

Many startups choose to host their sites on a shared server, mostly in an attempt to cut down on costs. This means that many other sites are running on the same machine and using the same set of scripts and programs. You can never control the way others are using the server. The overall setup becomes very vulnerable as hackers get a lot of gateway options to exploit. Therefore, if you can afford it, always choose a dedicated server over a shared one.

2. Check frequency of security updates and patching

A good hosting company always makes sure that they are running the latest versions of all programs and implements security patches as soon as they become available. So ask your hosting company how often they check for software upgrades, and how soon they apply patches as they become available. You are usually better off with a well known hosting company as they understand the risks associated with late patch applications and outdated programs.

3. Control and log data access

Always know who has access to your data. Keep a log of all data modifications so you know who accessed your data, and

when the changes were made. Protect your access information and share them only with the employees who really need them. Implement a Change Control system which will help you with versioning and tracking. Some good change control systems are Freshservice, Change Gear Change Management from SunView Software and Salesforce.

4. Ensure data and server's physical security

In one of the largest data centre outages known to date, thousands of websites went down, some going down for several days as The Planet's data centre in Houston was affected by an explosion and electrical fire in 2008. The physical safety of your server hardware is as important as the security across the network. Is your server room secured? Can somebody run away with a hard drive? Ask these questions and restrict access to the server room. If your server is provided by a hosting company, inquire about their policies regarding on-site security.

5. Activate https - Use a SSL Certificate

A SSL certificate is a small data file activated in the server that activates the padlock and the https protocol. Https authenticates the user's connection with the web site and the associated server. You will see SSL certificates being used on most banking and commercial sites. Users are more comfortable providing information like social security number or bank details on sites implementing a SSL certificate.

The process of moving your site from http to https must be done with great caution though. According to Garen Arnold, author at the hosting and web security review site tbwhs.com, there are two core types of problems firms often face when the transfer is not carried out well.

First is the SEO implication. Your site might lose ranking and face indexing issues if the current URLs are not mapped into the new ones correctly. You will also have to do a lot of 301 redirects, and point your backlinks to the new domain whenever possible. Even after your move is done, you should monitor your site for several days to look out for crawling and indexing problems and make sure that the traffic hasn't dropped.

Garen says that the second issue is related to the type of SSL certificate you buy. Measure your options and buy the right type of SSL certificate. You can buy an SSL certificate at a yearly price of anywhere between $10 and $500. They offer different kinds of protection and might secure a single domain or multiple domains with unlimited sub domains. Comodo PositiveSSL and Geotrust RapidSSL are two cheaper options costing around $10/year that even the most cash-crunched startup can afford. (If you can't find the least priced options on their websites, try getting them through Namecheap).

Whatever you choose, confirm that your SSL certificate is widely accepted and supports all the major browsers. When not accepted widely, the SSL certificate in effect could be identified as a malicious threat by your user's browser in some cases.

6. Always encrypt user data on disk

How are you handling your user data? If you are storing data in databases, activate database encryption. If you are writing on text files, consider using an on-the-fly encryption tool. BitLocker and VeraCrypt are two free solutions that are very popular among professionals.

7. Implement monitoring for your site

Monitoring for your site regularly is very important. Utilise a web security monitoring service like Alertra, Pingdom or Sucuri to make sure you get to know about any downtime or security breaches in your system as soon as they take place.

ABOUT CHARLES MBURUGU

HubSpot-certified content writer/marketer for B2B, B2C and SaaS companies. He has worked with brands such as GetResponse, Neil Patel, Shopify, 99 Designs, Norton, Salesforce and Condor. Portfolio: https://charlesmburugu.contently.com/ LinkedIn: https://ke.linkedin.com/in/charlesmburugu

- Telltale indications that your WordPress site been hacked - 2 Jan 2018
- Are you making these WordPress blunders? - 17 Jul 2017
- Tips for maintaining your WordPress business site - 25 May 2017
- Selecting a domain name: blunders to avoid - 3 Jun 2016
- Four Windows server backup solutions - 23 Dec 2015

View my profile and articles...