9 tips to protect your CRM data from malicious hackers

By Erika Morphy

CITEworld | Sep 23, 2014 6:00 AM PT

It turns out that Home Depot was shockingly lax with the security around its customer data, according to a news report in the New York Times this weekend. How bad? Security workers at the retailers took to warning friends to only use cash when shopping at the store.

There didn't seem to be any one particular reason why Home Depot was so slow to make the changes it should have, but rather several factors combined with (as I imagine) a sense of being overwhelmed by the task ahead. No matter: Assuming the report is accurate, Home Depot's position is inexcusable. Retailers have been in the crosshairs of hackers for years now and it should have known.

Right now the headlines are focused on the cyber vulnerabilities of national retailers but another threat is looming -- one aimed specifically at CRM systems.

A few weeks ago, Salesforce notified its customers that that the Dyre malware, which typically targets customers of large financial institutions, has been tweaked to target some of Salesforce users as well.

This malware is not targeting a vulnerability within Salesforce's platform; rather, it resides on infected computer systems and steals user log-in credentials. Presumably, it can piggyback its way into a corporate system using any CRM application. And once it gains entrance, all sorts of low-hanging fruit await: Payment information, customer data, and possibly sensitive intellectual property of customers. There is also a wealth of knowledge about company relationships and who controls the purchasing power.

"Often CRM systems will keep the contact information of C-level personnel from other organizations that a company is doing business with," David Pack, director of LogRhythm Labs, says. Using this information, "a realistic-looking spear phishing e-mail can be crafted, turning this into a potential supply chain attack on other organizations that might not even be Salesforce users."

Scared now? Good. Here's what you can do about it.

CITEworld spoke with several security experts to see what steps a company could take to protect its CRM data specifically. We began with a few base assumptions, namely that the fundamentals were in place -- assume your security software isn't outdated, and the security team has access to all networks including customer data (both reported to be Home Depot's failings). We also assumed more advanced -- but still commonly cited -- protections are in place, such as two-factor authentication.

In other words, we asked what *else* can companies do to protect their CRM data? This is what we learned.

Understand the scope of your task

Or as Tom Cruise said in the first Mission Impossible movie, "relax, it's much worse than you are thinking."

Understand that you are most vulnerable to a "man in the middle" attack vector, said Kyle Kennedy, CTO of STEALTHbits Technologies.

"The sad part is that when this happens everyone will blame the service provider even though it's typically the fault of a careless employee at a an organization consuming the service who either decided to use his infected home machine to interact with the company's data, or the individual that foolishly clicked a hyperlink that results in malware being installed on his business machine.

Don't stop reminding employees and partners of the risks

The best way to counter the risk of these attacks is an extensive and ongoing social engineering education campaign with employees and partners. "Make sure everyone knows that an authorized tech will never ask for things such as passwords," according to Andy Pace, Chief Operating Officer of SingleHop. "Also employees should know not to access your CRM through emails from unidentified senders."

Know that protecting the data is more efficient than protecting the boundary/container

Given the propagation of data in business workflows, protecting the data itself over its lifecycle protects it from advanced threats, says Trish Reilly, who handles cloud product marketing for Voltage Security.

"Containers only protect data at rest -- which only shields the data from a very narrow set of threats. In today's cloud, advanced threats attack data in use, in motion, and at rest -- which points to using a continuous data-centric approach to mitigate them."

Encrypting the data at the container has value if used as a means to protect it in the event of media removal, theft, recycling, she continued. "If the concern is to protecting data and its movement (or unknown movement) then encrypting higher up -- at the application layer through a data-centric approach -- is safer," she said.

Choose encryption wisely

With the rush to protect data in the cloud, many solutions have emerged that make serious trade-offs with security, such as enabling searching and sorting by weakly encrypted data, Reilly also noted.

Enterprises need to choose vendors that have validated, secure methods with independent validation, she said.

Have clear auditing and visibility in place

Administrations need to have a clear understanding of who performed which action, when, from where, using what device, says Boris Gorin, head of Security Engineering for FireLayers.

"This is critical to detect any abnormal behavior, like, say, an "administrator" logging in from China in the middle of the night, as well as conduct forensic investigation in case any potential or actual breach is suspected."

Think "need to access"

Make sure each user only has access to the information they need. This will limit exposure of customer information.

Also never have group accounts; accounts need to be separate and established for each user, says SingleHop's Pace says. "This allows you to ensure accountability and makes it easy to isolate breached accounts."

And add VPN and IP range restrictions where applicable, he adds. "Many users only access CRMs from the work place and each of these users should have their access limited to VPN."

Get proactive with DLP

IT can prevent malware incidents by using Data Loss Prevention (DLP) at the endpoint level, says Roman Foeckl, CEO of CoSoSys.

"DLP technologies should be combined, meaning they should be used to protect data in motion, DLP for data at rest and DLP for data in use," he says. "Scanning data at rest is useful to proactively determine what endpoints are particularly vulnerable based on large amounts of CRM data residing on them."

Ditto mobile endpoints

Mobile endpoints -- smartphones and tablets -- also need to have an MDM solution in place since lots of CRM data and access credentials are saved on them, Foeckl added.

Ensure proper data backup and recovery solutions are in place

Jeff Erramouspe, CEO of Spanning, says that most of the Salesforce administrators the company has met are either doing nothing specific to protect their data, or at most use the Salesforce Weekly Export feature. "Automatic daily backups are needed to ensure IT-level business continuity in case the worst does happen," he says.