FINANCIAL TIMES

http://www.ft.com/intl/cms/s/0/b4807a14-5097-11e4-8645-00144feab7de.html

Hackers find suppliers are an easy way to target companies

By Hannah Kuchler
The Financial Times
October 20, 2014

The windows may be bolted and the security gate locked, but security experts are warning that unless every other entrance and exit is secured, cyber criminals can still enter your company via your supply chain.

The risk of hackers entering a company's computer networks through a supplier – or even, the supplier of a supplier – has become a greater concern since the cyber attack on the US retailer Target late last year.

The details of more than 70m customers of the food-to-clothes chain were compromised, including the accounts of more 40m credit card holders, snatched by a criminal who entered the system using access granted to a refrigeration and air conditioning supplier.

Craig Carpenter, at AccessData, a computer forensics and cyber security company, says a whole range of suppliers, from vendors to law and accounting firms, have often been used by cyber criminals looking for an easy way in to a company's databases.

"Financial criminals will typically look for the weakest link – the most efficient, easiest way into a system. And, the majority of the time, suppliers are the easiest way in," Mr Carpenter says.

There is no such thing as "perfect vendor management", says Rohyt Belani, chief executive of PhishMe, an email security company. He says cyber criminals are becoming more creative in how they target individuals to win their trust and enter their computer systems, for example, studying the social media profiles of suppliers' employees to understand what will make them click on an infected attachment, a technique known as spearphishing.

He says these are not the typical sort of phishing methods people are used to, "sending you emails offering you $20,000 that even the untrained [are] not going to act on. Spearphishing is the attackers sharpening their pencils and doing reconnaissance."

Smaller companies often have less to spend on sophisticated cyber security, as shown by a recent survey by professional services company PwC that showed budgets for security fell 4 per cent last year, led by the decline in small company spending. This is despite an overall rise in the number and complexity of cyber attacks.

One reason for this is smaller businesses often have less negotiating power with service suppliers that offer more protection, such as Amazon and Rackspace, which are reluctant to change standard contracts for all but the biggest customers, Mr Carpenter says.

Sam King: 'Every company is becoming a software company'

Sam King, executive vice-president of strategy for Veracode, a cloud security company, warns that "every company is becoming a software company" and says businesses often do not realize how dependent they are on third-party software until it is too late.

For example, this year, the US hardware store chain Lowe's suffered a security breach affecting employee information including social security numbers and driving records, which was stored in an online database provided by a supplier that did not properly secure its back-up copy.

Ms. King says boards are just beginning to realise what a complex web their sensitive information is stored in and how important it is to vet suppliers.

Vetting is a constant process, she says. "If you list the top-10 critical suppliers and make sure they are secure, then that list might change or some random website created by a third party that wasn't in the top 10 may be the risk."

Ionic Security, a start-up in Atlanta, Georgia, suggests it might have the answer to securing data wherever it travels in the supply chain. Its encryption method cocoons a piece of data in a protective layer that calls back to the company that owns it to ask for permission every time it is opened, and tracks who uses it and how.

Adam Ghetti, Ionic's chief technology officer, says many "early adopters" using the software are trying to mitigate supply chain risk. He has customers in financial services, energy and manufacturing. Any industry that is highly regulated, has a broad distribution base and relies on many vendors needs to consider its supply chain security, he adds.

Mr Ghetti says that supply chains do not have to be very big to be at risk: where the data go to may be more of a problem.

After the Edward Snowden revelations last year, which exposed a National Security Agency mass surveillance programme in the US, some companies have been especially cautious about letting their data travel to territories where it might be spied on.

Mr Ghetti says: “The [uses] we’ve seen are companies working with suppliers in a particular region who want the information they exchange to stay in that region.”