

FINANCIAL TIMES

If Google can be hacked, is anyone safe?

Businesses pour millions of dollars into a never-ending “virus-antivirus” arms race, all the while wondering: “If the technology titans can be hacked, what are the chances that my data is secure?”

IT sophistication means we can now watch individual data packets as they enter and exit systems; we can scan files for known viruses, as well as those yet to be written; we can examine corporate networks to see who’s online, what they’re doing and how they are doing it. Yet we are still vulnerable.

At the heart of this insecurity is the “zero-day exploit”. It is derived from a programming concept that refers to day one of a software development project; known as the zeroth day.

Thus, a zero-day exploit takes advantage of the window of time between when developers are made aware of a problem and when the complete software fix can be developed and distributed.

Zero-day exploits, by definition, are vulnerabilities that have not been addressed by hardware and software manufacturers. Thus, there are no virus signatures to be downloaded or software patches to be updated, leaving the bad guys with the upper hand.

Add to this the complexity and sophistication of today's attacks and it becomes easier to understand why industry giants such as Google can be hacked.

Recent reports indicate the Google attacks started on social networking sites. The attackers watched key Google employees to identify their friends and associates and hacked these accounts.

Then they used information gained to contact other employees and, appearing legitimate, lured unsuspecting victims to nefarious websites, which provided the doorway through the company's firewall.

These attacks have become known as "chained exploits", a series of vulnerabilities and weaknesses that when used in tandem, can break even the most secure systems.

In another example, a corporation detected a calamitous virus infection which plagued more than 500 computers in its network. It thought it had dealt with it successfully but six months later the company identified suspicious traffic indicating the presence of another virus.

After forensic analysis, it was discovered the “new” malware had been installed during the earlier attack. Once the second virus was in place, it didn’t matter to the hackers that the first virus had been destroyed.

Chained exploits not only create new vulnerabilities, they can lead to a false sense of reassurance by allowing the first virus to serve as a decoy, leaving the impression that efforts to destroy the first virus have solved the problem.

So what can you do mitigate this risk? First, assume that no matter how good your firewalls, infections will happen from time to time. Maintaining diligent and timely patch management of applications, operating systems, and network devices is a must - but not sufficient.

Where possible, restrict access to sensitive information to as few people in the company as possible – that way a breach of one person’s computer, won’t open the keys to the kingdom.

You also need an emergency response plan in place before a virus attack to assess whether it is the sort of attack that can be dealt with using commercially available virus detection software (which will be true in most cases), or if the infection is systemic or is affecting an especially sensitive system that constitutes a breach of your central infrastructure.

In that case you might need to decompile the virus’s code to understand exactly what it did, how it operated, and seek expert advice on finding and containing the damage.

The recent cyber attacks also reveal a changing motive - the hackers wanted to steal intellectual property or corporate secrets. Indeed, some recent hacks involved viruses that automatically copied every email sent or received by key individuals to a shadow address, giving the hackers a clear view of the company’s secrets.

In short, this new wave of hacking is corporate espionage. The implication is clear: previously, the financial risk of hacking was primarily of damage to a network and perhaps reputation. Now the risk is far greater – the new target is the business information upon which a company relies.

Stroz Friedberg provides digital forensics, incident response and electronic disclosure in the UK and the US. Seth Berman is a managing director in its London office; Lam Nguyen is a director of digital forensics in its Boston office.

This article was published on the Financial Times website, 5 March 2010.