Cyber security: The threat to governments and business

John Hawes

Hacking and malicious software have become very real and very serious threats to consumers, businesses and governments alike. When this is combined with the increasingly complex international cybercrime investigations and prosecutions, the growth of as yet unregulated ‘crypto-currencies’ such as Bitcoin and a growing awareness of privacy issues among the general public, there is a lot for governments to do to ensure they are properly addressing the issues of online security and safety.

Malware and cybercrime affect us all

The year 2014 was a bumper one for cyber threats of all kinds, and 2015 is likely to bring further breaches at major corporations and institutions. With the internet underpinning an ever larger proportion of our communications, entertainment, banking, commerce and interaction with public service providers, anything that dents our confidence in its security will reduce the uptake of cost-saving online services, just as it impacts trust in the organisations involved.

The hacking and malware threat has also moved firmly into the political arena, with numerous incidents of data-stealing software targeting politicians and government institutions discovered and blamed on nation states in the last few years.

At least one major threat, the Stuxnet worm – which, discovered in 2010, targets nuclear processing equipment in Iran – is now generally believed to have been orchestrated by Western government agencies. Over the last few years most national disputes have spawned at least some form of online offshoot. While so far these have mostly been little more than digital vandalism and propaganda, such as the social media compromises routinely perpetrated by the ‘Syrian Electronic Army’, there have been indications of more serious attacks targeting critical infrastructure.

There are also indications that government-sponsored hackers are targeting foreign business interests as well as spying on foreign diplomats, with both the USA and Canada openly accusing China of industrial espionage in 2014. Relations between the USA and North Korea were heavily strained throughout late-2014/early-2015 after a cyber-attack on the systems and data of Sony Pictures Entertainment led to extensive leaks of sensitive data and pressure on the firm to suppress one of its films. This attack was widely claimed (including by the FBI) to be the work of North Korean hackers.

All this means a lot of effort is required of governm ents around the world, from a number of angles, to keep the heavily relied-upon online world from collapsing under the weight of fraud, theft, impersonation and improper access to protected systems.

Consumers need to be reassured of the relative safety of conducting their lives online, educated on how to improve their safety, and shown how to deal with incidents of fraud and impersonation. Businesses need to be regulated and monitored to ensure the proper efforts are being made to protect corporate networks and the data held on them, which often includes highly sensitive information on clients and customers and also, in some cases, sensitive internal information that may be of interest to rival businesses. Perhaps most importantly, government bodies designing and implementing digital services need to ensure the highest standards of security are built in from the start.

Governments need to store vast amounts of information on the people, organisations and businesses under their aegis. Much of this information is highly confidential and sensitive, and any leak, loss or misuse of this data can be hugely damaging both to the institution holding the data and the individual or body to which the data relates. Health services are particularly at risk, given the combination of extremely sensitive information and the need for rapid access in emergencies.

At the other end of the scale, governments need to operate critical infrastructure such as power generation and supply, waste removal and disposal, and transport. These areas are also increasingly controlled by computers that are, in turn, increasingly connected to the internet for centralised operation and monitoring, which puts the stability of infrastructure at great risk should those computers or the communications between them be compromised by malicious actors. Military resources and activities are similarly delicate targets for both espionage and terrorism.

Outdated and vulnerable authentication methods

One of the major issues underlying all these problems is authentication: the way we confirm people are who they claim to be when granting access to information systems and services.

In the flesh-and-blood world, many institutions still rely on outmoded methods of identifying people, such as signatures, social security code numbers (SSNs) or the possession of ‘official’ paperwork such as utility bills as proof of address. We also continue to treat bank account and credit card numbers as secrets that should only be known by their proper owner. Similarly, online we mostly depend on simple usernames and passwords to access accounts of all kinds, and traditional backup methods relying on personal information (‘mother’s maiden name’, ‘name of your first pet’ and so on) are also highly dubious in a world where vast amounts of information on just about anyone can be dug up in moments.
If the data leak explosion of 2014 has proved anything, it is that these methods can no longer be trusted. Signatures have never been easy to definitively prove or disprove, while advances in scanning and printing technology have made forgery of supporting documentation cheap, fast and simple. Supposedly private information, such as social security numbers or card numbers, have been leaked in their billions over the last few years, in many cases with the associated usernames and passwords attached. Several major data breaches, such as the Adobe leak of late 2013, have affected hundreds of millions of online accounts in a single instance.

It is therefore imperative that we find a better way of identifying ourselves and our citizens, clients or customers. Guidelines released in late 2014 by the European Banking Authority recommend ‘strong customer authentication’ for all online commerce transactions by mid-2015, defining this authentication as two of the three standard pillars of two-factor authentication: ‘Something you know, something you have, something you are.’ If this becomes standard in e-commerce and banking it is almost certain that all other areas of online authentication will follow suit.

Biometric techniques, the ‘something you are’ component, use features of our bodies, such as fingerprints, eye patterns, voice tones and facial features, among others. Implementations of these measures continue to evolve and become more usable, with at least two major projects working on standardising and unifying various approaches, but these all require some sort of technology to read the data from the physical world and convert it into digital information. This will inevitably be more expensive than simple signatures or passwords. Furthermore, with so many approaches being developed there is still no sign of a single universal method emerging. Add to this the remaining problem of theft and impersonation – while a leaked password can be changed, it’s considerably harder to change one’s fingerprints – and it seems unlikely that biometrics will become a universal solution, at least in the near future.

The most widely used alternative form of second-factor authentication, one-off codes sent via SMS or generated by dedicated devices or smartphone apps are more likely to be viable on a large scale in the short term, but these are also subject to interception or manipulation. Android smartphones in particular have become a major target for malware, much of which tries to sit invisibly in between phone users and their banks to steal credentials, spoof or steal one-time codes, and hijack banking sessions. These systems require some effort to implement but are becoming more and more available to web developers in the form of simple ‘plugins’: pre-built modules which can be added to standard website building systems. This in itself may present a further danger, as poorly implemented or misconfigured systems can lead to flawed and unreliable authentication. They also require access to a phone or code-generating device, but compared to biometric readers these are much simpler, cheaper and more widely used by the general population, with many banks already deploying some form of one-time code system. It seems likely that, within the next year or so, many governmental bodies will need to deploy this sort of approach to properly authenticate people accessing their services online, with everything from tax filing and voter registration to health and welfare services open to abuse if not properly secured.

Addressing the issue of cybercrime

The steady increase in both malware and cybercrime has highlighted the need for cross-border co-operation and operation and information sharing to assist in tracking down those behind digital crimes and bring them to justice. The availability of ‘bulletproof’ hosting services in some regions makes crooks feel immune to the justice systems of the nations they attack; as such diplomatic efforts to eradicate these safe zones must continue.

As well as prosecuting criminals, there is a great need to better regulate how attacks and compromises are recorded and measured, since the scale of the problem is still obscured by a lack of detailed and reliable information. While breach notification laws continue to evolve, the reporting of online crimes remains limited, impeded by lack of clarity on who to report such incidents to and, in many cases, considerable unwillingness on the part of victims to own up to losing control of systems, data and, indeed, money.

Once the current swathe of problems linked to online security is mopped up, there will remain much to be done to limit future issues. Last year revealed several severe issues in the basic underpinnings of the internet itself, most notably ‘heartbleed’ and ‘shellshock’ vulnerabilities, as well as the regular security flaws in just about every commonly used piece of software. To keep us from suffering further shocks in the future it is imperative that regulators, buyers and users put pressure on software developers, both commercial and open source, to implement better practices to reduce the frequency and severity of such problems, and to build security into everything from the very start.

As the ‘internet of things’ brings online connectivity to household equipment, the penetration of computer networks into our everyday lives grows ever deeper and the need to keep them safe, reliable and secure becomes paramount.

Endnotes


Virus Bulletin conference

The 25th Virus Bulletin International Conference (VB2015) will take place from 30 September to 2 October 2015 at the Clarion Congress Hotel in Prague, Czech Republic. The VB conference is the premier anti-malware and IT security conference, at which the brains of IT security from around the world gather to learn, debate, pass on their knowledge and move the industry forward. The event provides three full days of learning opportunities and networking with industry experts, and covers all aspects of the global threat landscape.

JOHN HAWES is chief of operations at Virus Bulletin, the leading online publication on malware and computer security, where he has been running the world-renowned VB100 certification scheme for anti-malware solutions since 2006. He also sits on the board of directors of the Anti-Malware Testing Standards Organisation (AMTSO) and the board of managers of the Clean Software Alliance, and is a regular contributor to the Naked Security blog.