Obstacle course

The protection of IT networks from criminal attack can often fall at the first obstacle – the web browser. Stefan Frei of the Swiss Federal Institute of Technology tells Jim Banks that there is an insecurity iceberg standing in the way of accurate risk assesment at a time when organised crime is becoming a significant online threat.

According to a recent study by the Swiss Federal Institute of Technology (ETH Zurich), nearly half of UK employees are thought to be at risk of data theft at work. This statistic should worry any organisation, and can only encourage the efforts of those who seek to steal personal, confidential and valuable data.

The study, backed by IBM and Google, reveals that 45% of internet users do not keep their browser – whether it is Internet Explorer, Firefox or any other – updated with the latest security patches. This means around 600 million users worldwide have out-of-date browser security, which the researchers feel is a recipe for disaster, given that websites are a key point of entry for cybercriminals. No one should be in any doubt about the potential level of risk to a company's reputation, brand and financial position that arises from inadequate network security. Finance directors must recognise that a security breach – and the fraud that might follow – could seriously impact the bottom line.

'There is an insecurity iceberg,' says Stefan Frei of ETH Zurich. 'We can only measure about half of the risk. Ten years ago it was just techies looking for weaknesses in online security, but now the threat is from organised crime, which is behind many attacks.

'The risk is real. On the black market you can buy credentials to access bank accounts. There are gangs specialising in technology. Furthermore, the risk is growing. Technology development happens very fast – much quicker than we can absorb as humans. For now, the threat is moving ahead faster than our defences can match.'

As well as bogus websites or phishing emails that seek to gather personal and financial data, sophisticated cybercriminals can in some cases cooperate to simulate a legitimate company. The threat is international and involves a variety of different software systems, with the result that not only is the threat more sophisticated, but also there are more open doors out there. Just as an open window invites a burglar, a weak online security system draws hackers. Furthermore, the information held by the finance function is the richest target.

'The attacks are automatic and systematic, searching for vulnerable machines,' Frei remarks. 'The enemy is professional. In our research we looked at why attacks are successful and found that there is a very large population of vulnerable machines. This opens the door to mass-hacking of web servers, and there are problems with the complexity of networks and security measures that result in the loss or theft of data.'

Frei also sees more vulnerability from outdated browser plug-ins. His conclusion is that simple measures such as installing software updates can have a significant effect, but at present the process to ensure this happens is often unclear.

Browser update

There are, of course, many steps an organisation can take to protect its data. Very sensitive information may need to be stored on segregated machines that have limited or no access to the Internet or email.

'If you have very sensitive data then you can remove email capability from the machine that houses it. You can separate it either physically or virtually. The important thing is to find the right working point for your environment,' says Frei.

Installing web browser updates and security patches is a relatively simple process and can greatly improve overall network security, but organisations need to define where the responsibility lies for ensuring software is up-to-date.

At present, individual users generally shoulder the blame, but Frei believes that this is unfair. The users cannot face a growing threat alone, so a clear process and a clear chain of accountability are needed to support them.

'Users are not in control of updating software. The industry is flawed but users should not get the blame,' stresses Frei. 'Instead we have to collaborate. Vendors must cooperate with users, though it's hard to get them moving. Online criminals already collaborate, so a bank, for instance, cannot cover all the threats on its own.'

Coordinating the efforts of vendors may be easier said than done. A single browser may have up to ten plug-ins to enable functions such as reading specific file types or playing different media, which may come from different vendors. There are, therefore, many separate updating procedures to be performed. Finding ways to simplify these updates could make a big difference, but again awareness and accountability are the key issues in balancing a corporate's responsibilities with a new approach to systems development.

'There are some security measures that are beyond the reach of the lone user, but the company can invest in them. Also, the software has been developed by geeks, who don't behave in the same way as most users. There has been too much focus on the geek mind, so we need to test how software is used, which takes us into the emerging field of the psychology of security,' says Frei.

To improve awareness of security, Frei believes it is important to understand users' attitudes in order to devise methodologies that ensure they pay more attention to updating software and protecting data. Finance directors should play a key role, given their guardianship of the bottom line and the sensitive data that resides in their department's systems.

The psychology of security

As Frei observes, the world of business and finance has too many security solutions aimed only at geeks. He and his colleague Dr Martin May are trying to understand the implications of this, and are developing an approach based on user psychology as an antidote to the 'fly it, break it, fix it' mode of software use that normally prevails.

'Security is very interdisciplinary,' says Frei. 'It needs all the elements of education, psychology, technology and leadership working together.'

'We point out that security breaks are at the weakest part of the chain. The people who write the code are very different from the people who use the code,' agrees May. 'Normal users are more prone to phishing, for example, than users who have a higher level of knowledge about internet technology.'

One idea that has already emerged from this approach could radically influence attitudes

'Ten years ago it was just techies looking for weaknesses in online security, now the threat is from organised crime. The information held by the finance function is the richest target.'

The insecurity iceberg

Using passive evaluation techniques, ETH Zurich identified the online community at risk due to a lack of the latest version of web browsers.

Estimated users at risk:	
Internet Explorer	577 million
Firefox	38 million
Safari	17 million
Opera	5 million
Estimated total at risk:	637 million
Estimated total global online community	1,408 million internet users worldwide

Threats to browser security

- Web browsers and plug-ins have vulnerabilities. Plug-ins are hard to patch
- Browsing patterns can be unpredictable
- 'Drive-by' downloads – popular, high-traffic websites seeded with malware can spread infection rapidly to vulnerable hosts
- Growth in drive-by download has resulted in many websites suffering mass defacement, including sites run by the UK Government and the UN
- Google has uncovered over three million malicious web addresses that initiate drive-by downloads
- Spam emails may contain URLs directing victims to web servers hosting malware
- Malware is often in the form of Trojans, pieces of software that appear to perform a useful function

towards network security. Borrowing from the food industry, Frei and May suggest that a 'best before' date on browser software and plug-ins would at least help educate companies and users about the need to update their browser.

Their research has identified that, in most cases, the absence of critical or important updates to web browsers is technological, motivational or informational. Users either can't do it, don't care about it, or don't know it needs to be done.

Almost all users are familiar with the concept of 'sell-by' and 'best before' dates on perishable goods. A 'best before' date for all new software releases would encourage users to patch or refresh their applications, while online businesses could use it to help evaluate or mitigate the higher risk of customers using out-of-date software.

'It is a mechanism that people know from food shopping and it would address a core security issue. If you see web pages indicating the need to use the latest version of a browser then you know it is time to refresh. The highest potential is on the banking side, or any site that uses sensitive information,' says May.

'Banks could inform users about the risks of older browsers, and could enhance the security questions to log in if the browser has not been updated,' adds Frei. 'If you have an updated browser, the log-in process would be quicker. Alternatively, banks could apply different terms and conditions for the use of older browsers.'

Although there is much more research to be done, particularly as threats to network security evolve, one message is clear: the current approach to security in the web browser space would fail by the safety standards set in many other industries, and it is time for that to change.

'You can give out a flawed piece of software, but you can't put a car on the road that is not safe,' warns Frei. 'We accept software of a quality that we would never accept in other markets. We always want features, not security. As a result, security is not prioritised and not appreciated until it is too late.'

He remains, however, optimistic about the future, provided that the business world heeds the warning and responds by committing to what will be a long battle against cybercriminals.

'We are still at a very early stage in technology development. Just look at how cars have changed over the years,' Frei says. 'Companies should be able to choose the risk level at which they want to work, but at the moment that level is too high. However, we will survive. After all, there is shoplifting, but we still have shops.'

The FD has to be involved in the discussions that set the risk level and must understand that security of corporate financial systems is not just an issue for the IT department. ■

'Security... needs all the elements of education, psychology, technology and leadership working together.'

Author

Stefan Frei is a lecturer and security researcher at ETH Zurich. Before that he worked in the ISS X-Force to provide technical expertise and security consulting for international clients around the world.

Most secure browsers

Looking at the latest official public releases of web browsers as of June 2008, ETH Zurich was able to compare their levels of security. Internet Explorer 7 (IE7), Firefox 2 (FF2), Safari 3 (SF3) and Opera 9 (OP9) were the benchmark versions.

The share of users for each web browser using the latest major version as of June 2008

Latest web browser version	IE7	FF2	SF3	OP9	Total
Release date	18 Oct 2006	24 Oct 2006	26 Oct 2007	26 Oct 2007	
Share of users with latest version	52.50%	92.20%	70.20%	90/1%	59.10%
Number of users with latest version	579 million	209 million	34 million	Ten million	832 million

Source: ETH Zurich (www.techzoom.net/insecurity-iceberg)

- Globally, only 59.1% (832 million users) had the latest major version of their preferred web browser
- On any day in the first half of 2008, 83.3% of Firefox users, 65.3% of Safari users, 56.1% of Opera users and 47.6% of Internet Explorer users were using the most secure version of their browser software
- 16.7% of Firefox users continue to use outdated versions, despite the single-click, integrated auto-update function

Top ten information security tips for c-level executives

1. Businesses need to create and maintain a comprehensive corporate information security (IS) policy. This should be supported by related guidance, including detailed policies and procedures, on how to deal with IS issues. This policy should be closely aligned with business priorities. Senior management needs to endorse the approach and show total commitment to IS, stressing the need for good communication, comprehensive awareness of the key issues and compliance with relevant regulations.
2. Management and staff must have a common understanding of the importance of security issues together with key IS requirements, vulnerabilities and threats. They also need to understand and accept their own security responsibilities and ensure that they have a confirmation process in place.
3. A corporate IS function should be established to manage the IS regime (ISMS – IS Management System), especially with respect to incident management and response.
4. A risk management policy needs to be established to define risk limits and risk tolerance and to ensure that clearly structured roles and responsibilities for risk management ownership and management accountability are in place.
5. Critical infrastructure components should be identified and continuously monitored.
6. Service level agreements (SLAs) should be used to raise awareness of, and increase cooperation with, suppliers relative to security and continuity needs.
7. Applications need to be secured well before they are deployed.
8. C-level executives should be aware that although insiders continue to be the primary source of most security risks, attacks by organised crime and from other external sources are increasing.
9. Proper attention needs to be paid to those legal and regulatory requirements that affect the business (e.g. data privacy, copyright and internal control demands).
10. The organisation's IS policy should be properly enforced through compliance and a process of internal and external reviews.

Source: John Morrison, MD, Sapphire