PROFESSIONAL SERVICES FIRMS - A SOFT ROUTE TO THE HACKERS' REAL TARGET?

Submitted by: Nuvias (Wick Hill)
Tuesday, 18 August 2015

Feature by Ian Kilpatrick, chairman Wick Hill Group

All companies today are at risk from a successful attack on their IT systems. It's widely acknowledged that it's no longer a question of if you will be breached, but when. Unfortunately though, some companies are more at risk than others and are actually being selectively targeted.

Larger companies and enterprises normally having bigger security budgets and bigger security teams, resulting in stronger core defences, so hackers are looking for soft target entry points into these systems.

Professional services organisations such as law firms, accountancy and audit firms, management consultants, M&A advisers and recruitment companies are now being targeted because of the valuable and confidential information which they may hold on their clients, and more importantly, because they can provide a back-door entry into those clients' systems.

Retailer Target was hacked, lost data on 70 million customers and, in direct consequence their CEO, through a focussed breach of one sub-contractor.

While larger professional firms tend to have robust security and large IT security teams, many mid-range and boutique organisations are still struggling to play catch up. With the increased range of attack vectors being used, it is important for secondary targets to ensure that they have protected both their perimeter and their key data.

For those relying on indemnity insurance for protection, it is worth reviewing the policy to understand exclusions, and more importantly to recognise that even if indemnity covers the initial impact, it won't cover the reputational damage and future financial impact.

While aware of the threats and risks, many professional services firms are not using the same degree of penetration testing, security analysis and security defence as that used by their clients, and not with the same degree of focus.

With a number of recent breaches raising the profile of this risk area, enterprises are increasingly carrying out risk analysis on their professional suppliers. At one level, that covers supplier access rights into their networks, but we are also seeing professional services companies being required to prove their data security.

For customers, the first easy test of how serious suppliers are about security is to ask if they have strong two factor and network access authentication, and data encryption – including at the partner level (the people with the highest levels of access, but often the lowest desire to follow the security rules). A 'No' to that question should raise serious alarms about whether or not you should provide that supplier with access to your company networks confidential company information, or indeed the

ability to send emails to senior staff (opening emails from a trusted supplier is one of the easiest ways to penetrate an organisation).

Last year, whistleblower Edward Snowden urged lawyers, journalists, doctors, accountants, and others with a duty to protect confidential information, to upgrade security in the wake of the spy surveillance revelations. He said: “Unencrypted communications on the internet are no longer safe. Any communication should be encrypted by default.”

The security dangers for professional organisations is certainly an issue which is recognised by professional bodies. The Law Society says on its website “Cyber attacks are a threat to all businesses today and law firms are particularly attractive sources of information. Commercial data, IP information, and sensitive client data may all be targeted.” The Society actively promotes security and offers a wider range of advice and education to its members.

The accountants’ organisation the ICAEW, also acknowledges the issue and provides a ‘Cyber Security Resource Centre’ on its website. The resource centre is a focal point for ICAEW members looking for support in managing cyber risk.

Industry bodies are a good starting point for those keen to ensure the security of the confidential data they hold on their IT systems. Key security elements, however, should as a minimum include network access control, encryption (of data at rest and data in motion), and mobile device security, with monitoring and management reporting alongside these.

The threats are significant and real. There is not only an increased awareness but also an increase in calls for action. For example, in February, the New York Times reported on US Wall Street banks, and the big law firms that do work for them, getting together to share security information1 The New York Times also commented on the concern of law enforcement agencies over the vulnerability of US law firms to online corporate espionage because of their repository of company secrets, business strategies and intellectual property.

Also in the US, The Wall Street Journal reported that banks were demanding law firms harden their cyber attack defences. While it would be nice to believe that attacks are only in the US, clearly it would be naïve to do so. Seth Berman, executive managing director of Stroz Friedberg, commented that: “The failure of UK law firms to tackle online security is leaving clients increasingly vulnerable to attacks.”2

Despite this, there is still strong evidence that many organisations with responsibility for securing confidential supplier information, do not have the levels of protection to deal with concerted cyber-targeting. Nor, in many cases, do they have partner-level, focussed teams ensuring that this is an ongoing high-profile area of concern.
And, of course, by definition, those same organisations do not have any contingency planning for how they would respond if they experienced a drop-through breach that damaged a major client.

The one thing we can be certain of in security is that by the time something becomes a topic of awareness

and discussion. it has trickled down from high-end, individual, focussed attacks to a much more mass-attack route.

If you're providing data to your professional advisers, and it is market-critical or highly confidential, then it's clearly a good time to review their levels of security. It's also sensible to check on what security reporting they are able to provide you with to verify their security procedures are succeeding. For professional services providers, this is an opportunity for those who have strong security credentials to differentiate themselves from the many who currently do not.

Bio Ian Kilpatrick
Ian Kilpatrick is chairman of international value added distributor Wick Hill Group, specialists in market development for secure IP infrastructure solutions. Wick Hill supplies organisations from enterprises to SMEs, through an extensive value-added network of accredited VARs. In 2015, the company was named as one of '1000 companies to inspire Britain' by the London Stock Exchange Group. Kilpatrick has been involved with the Group for almost 40 years.

Kilpatrick has an in-depth experience of IT, with a focus on networks, particularly security. He has a strong vision of the future in IT, focussing on business needs and benefits, rather than just technology. Ian Kilpatrick is a published author and has written numerous articles and features, both domestically and internationally, as well as being a regular speaker at conferences, seminars and exhibitions

For more information about Wick Hill, please visit http://www.wickhill.com or www.twitter.com/wickhill

For press information, please contact Annabelle Brown on 01326 318212, email abpublicrelations@btinternet.com

ENDS

1. http://www.nytimes.com/2015/02/24/business/dealbook/wall-st-and-law-firms-weigh-cooperation-on-cybersecurity.html?_r=1

2. http://www.cyberriskinsuranceforum.com/content/law-firms-need-do-more-cyber-risk-0