SMEs bet on a cybersecurity CERT

CERT-UK has finally been unveiled, giving small and medium-sized businesses (SMEs) a powerful national ally in their defence against cyber-attack

CERT-UK could significantly improve the cyber-ecosystem for British SMEs

11:33AM BST 23 Apr 2014

The UK finally has a national computer emergency response team (CERT-UK) after the much delayed initiative was finally launched at the end of March.

CERT-UK – which was originally scheduled for last year but was put back because of recruitment and other issues – will co-ordinate responses to hacking and malware-based cyber-attacks at a national level. Some argue that its unveiling is not before time. US-CERT, its American counterpart, has been performing a similar role since 2003.

CERT-UK will become the first point of contact for UK businesses in relation to cyber-security issues. It will provide advice and guidance to help companies prepare and protect themselves, as well as expertise to help respond once an incident is reported. CERT-UK will also collaborate with other national CERTs, sharing technical information on cyber-attacks.

“We know government cannot do everything by itself,” said Francis Maude, Cabinet Office minister responsible for cybersecurity.

“CERT-UK shows we want closer co-ordination between government, business and academia to share insight and advice, as well as better co-operation with our international partners.”

The new body will be led by Chris Gibson, a former director of e-crime at Citigroup, who has chaired the international Forum of Incident Response and Security Teams for the past two years.

Mr Gibson said: “CERT-UK will build on existing arrangements for supporting the critical national infrastructure, and incorporate the Cybersecurity Information Sharing Partnership (CISP) which was launched last year and has proved extremely effective as a means of collaborating between industry and government.”

Larger businesses have all sorts of operational back-up in place; SMEs as a rule do not

It is expected that, for SMEs, CISP will become a focal point for up-to-date alerts and advisories on new cyber-threats. One of CERT-UK’s key aims over the next year is the expansion of the information sharing network, which currently has around 1,000 members representing some 400 companies.

SMEs in particular should be better protected after the advent of CERT-UK, according to cybersecurity experts.

Paul Lindsell, managing director of research company MindMetre, which regularly investigates attitudes to data governance, management and security issues, says: “Larger businesses have all sorts of operational back-up in place; SMEs as a rule do not, and tend to incur immediate and often substantial costs when their work is interrupted.

“So at the top level, an effective initiative that helps ensure that the infrastructural suppliers on which SMEs rely – banks, utilities, ISPs and so on – do not have service interruptions must be a good thing.

“The typical office-based small business – even the most obscure – will be experiencing several hacking attempts each week,” he says.

Mr Lindsell says there are some concerns about the new body, and he would like to see more overt co-operation between CERT-UK and existing anti-attack providers, including security software developers and specialist services for, say, factory systems security.

“On the other hand, if CERT-UK can become a true hub for sharing attack data and also be the source for more effective alerts broadcast to businesses large and small, preferably through the security systems they already use, then it would be of immense value and could significantly improve the cyber-ecosystem for British firms," he says.

While CERT-UK offers national co-ordination and leadership, UK industry remains responsible for its own cybersecurity. HP provides a state-of-the-art security strategy, tailored to the needs of SMEs, to help companies protect themselves against cyber-attack.