Europe’s banking system needs active management of cyber-security borders

By Chris Dye, VP Marketing and Communications, Glasswall

Trump, Brexit and the lingering after-shocks of the credit crisis – banking in Europe is under heavy scrutiny at the moment as it copes with all the pressure. Yet the wise heads concerned about the resilience of the banking system are also now focusing on cyber-security, with much discussion of how to use testing to prevent disasters.

Hardly surprising after the central bank of Bangladesh lost $81 million to hackers last year. The EU is considering tests and the European Banking Authority (EBA) too is increasingly aware of the risks of cyber-attacks, moving it to urge member states to take their own measures, while complaining that digital infrastructure is rigid and outdated.

Unfortunately, the problem is that the tests, if they ever are undertaken, will probably stick with assessments of the very same security techniques that are making banks vulnerable.

This is not a desirable state of affairs when banks, just like every other organisation handling data will face the full severity of the law after the European General Data Protection Regulation (GDPR) comes into force in 2018.

Under the terms of the GDPR, data breaches will be legally notifiable and costly, both in financial and reputational terms.

Yet European regulators are misguided if they imagine that concentrating on conventional passive anti-viral border security will provide banks with sufficient defence. Testing has to move beyond security architecture to encompass business processes and the establishment of best-practice approaches. The latter is difficult when information-sharing between national authorities is currently so poor.

What needs to happen is that banks completely reappraise their border security. Great claims are made about the effectiveness of conventional anti-virus and malware security, even though it is known to be ineffective against new methods such as Zero-day attacks. These are attacks that the anti-virus industry has not yet identified or categorised and does not have the technology to combat until it is too late. One of the leading cyber-security vendors this year claimed to have discovered “29 of the last 53 zero-day attacks”. If it only takes one bullet to kill you, the fact that 24 can get through to you is not much in the way of protection.

There is growing evidence that conventional anti-virus defences are no longer effective as hackers and cyber-criminals simply by-pass them. These standard approaches fail to address how the cyber-security world has changed. The great majority of malware attacks now start with an email to an employee. This will probably have been dressed up to look like it is from someone familiar to its recipient and contain a file attachment. Criminals will hide their malicious code inside a common file-type, increasingly using the actual structure of the file itself as a hiding-place. Conventional anti-virus solutions don't pick up these threats, but file-regeneration technology will.

The point about using file-regeneration is that it puts the power back in the hands of the organisation – in this case, the bank. Files are almost-instantly regenerated after being minutely inspected down to byte-level, validated against the manufacturers design specification and then rebuilt as clean, completely malware-free versions that are identical to the originals. Banks can then determine the levels of risk they want their various departments to be exposed to. Some pieces of code in documents which don't conform to the manufacturer's standard may be legitimate tools required for a particular task. The bank can decide what it wants to admit and who gets to use it.

This is best practice. Banks no longer have to rely on the dubious claims of conventional security vendors and can exchange documents with confidence. They don't have to succumb to the kind of fatalism that seems to have crept in across the cyber-security industry where the belief is increasingly common that your organisation will be hacked and you will lose data or be held to ransom. All you can do is to mitigate the effects.

Let's not forget how damaging attacks can be. The banking arm of Tesco was badly hit by cyber-criminals last November, with money taken from about half of the 40,000 accounts affected by "suspicious activity". It was serious enough for all online transactions to be suspended for a while. As well as having to refund its customers and rebuild its reputation, the bank is also likely to be stung with a humiliating fine.

Given the scope and sophistication of cyber-attacks, any stress tests ordained by the European Banking Authority or European Central Bank that focus exclusively on IT infrastructure and conventional anti-viral security are destined to be ineffective. It is time for testing to assess how a bank is embracing innovation to take the initiative against cyber-crime, managing an active policy that is adjusted to the precise level or risk required while shutting out all the malicious pieces of code that threaten the organisation's integrity and potentially, that of the entire banking system.