Client Alert

HANSUKE

Ransomware: No Surrender

Contact

Safdar Mirza
Cyber Security & Data Privacy
safdarmirza@hansuke.co.uk

Ahmed Nawab
IS Specialist
ahmednawab@hansuke.co.uk

Tel: +44 (0) 203 865 0625

Background

With the increase in the number of recent ransomware attacks, organisations are finding themselves in the embarrassing situation of having to inform their customers that they are unable to carry out their normal business functions due to being locked down by ransomware (a software that renders systems and data unusable until a payment has been made).

Banks and other financial services institutions are particularly vulnerable as their business models are based on trust which, if it falters, will have far-reaching consequences. A ransomware attack, if successful, results in loss of business, loss of earnings but most importantly may damage reputation beyond repair. The following are some practical measures to help contain a ransomware infection as well as to prevent any future cyber attacks.

Next steps

Under attack

If you are under attack, immediate action is required to limit damage and regain control. Take the following steps:

- Isolate systems – disconnect infected systems from network;
- Protect data – lock network drives and file servers;
- Assess extent of damage – search for .locky or similar extensions, and README files;
- Communicate with users – inform users how to remain safe and what activities to avoid;
- Identify source of infection – back track the first infection to ascertain the activity that triggered the infection;
- Restore data – restore data from backup; and
- Do not pay! – showing weakness will make matters worse. It will encourage criminals to continue exploiting vulnerabilities and cause even further disruption. Some instances have proven that payment does not guarantee the release of systems and data.

Post-attack

Once the incident is under control, taking the following steps will help to mitigate the risks from some obvious vulnerabilities:

- Immediately stop the use of obsolete or out-of-support software (e.g. Windows XP, Windows 8, Windows Server 2003);
- Patch all software and keep up to date;
- Use anti-virus and keep definitions up to date;
- Create backups; and
- Regularly restore test the backups;

Preventing future attacks

Taking the following steps will not only thwart ransomware related threats, but also help improve the general security posture of the organisation resulting in a security conscious workforce and a resilient work place:

- Build a strategy – it is critical to start from the top and build a strategy that helps set tone at the top as well as a vision that drives the direction of the organisation;
- Raise awareness levels – inculcate a security culture which in turn ensures security is everybody's responsibility;
- Automate – employ technology where possible to help carry out tasks that would otherwise be impossible to conduct manually e.g. security monitoring etc.; and
- Implement governance and assurance activities – embed proper procedures e.g. to manage incidents, carry out regular risk assessments and setup a Security Operations Center (SOC) to monitor threats.

How Hansuke can help

The expert team at Hansuke incorporates a deep knowledge of the issues that affect Financial Institutions. We specialise in providing bespoke and proportionate solutions to overseas and challenger banks. Our team consists of a unique blend of former Regulatory, Technology, Information Security and "big-4" personnel who will be able to assist you in with the end-to-end activities that will help you to demonstrate resilience against cyber attacks. We would be pleased to have a no-obligation discussion.

About Hansuke

Hansuke is an independent specialist financial services consultancy, providing truly independent advice. We are fully committed to delivering the right advice and solutions. This means that you get the optimal fit for your needs. We have assembled the right blend of expertise: spanning regulatory, information security, information systems and commercial financial expertise.