PREVENTION AND RECOVERY FROM RANSOMWARE ATTACKS

bluesource

Protect
Govern
Move
Manage

According to research by the global research organisation Wakefield Inc, two thirds of companies in Europe and America are now using on average 15 public cloud services and numerous shadow IT services, creating complex IT environments that are increasingly harder to configure and manage. Despite this, IT budgets have not increased sufficiently to cater for the change and are mostly unchanged, making it ever more challenging for IT teams to secure their environments and protect valuable company assets.

It is this perfect storm that has led to the material rise of ransomware attacks, with hackers using social engineering to successfully exploit broken perimeters, outdated technology, poor configurations and lack of user education.

The impact of ransomware is significant, with the latest figures showing that over 40% of companies have now been impacted. Furthermore, recovery times are now typically exceeding 5 days with costs averaging £200,000 per incident.

HOW WE CAN HELP

At bluesource we have the skills, tools and partnerships to help protect you from ransomware attacks and mitigate your risk. Some of the areas and competencies we can help with include:

IDENTIFY

Focused around risk profiling, defining robust processes and classifying data within your organisation and supply chains.

Products, partners and solution areas

- ✓ GDPR current state assessment
- ✓ Data Insights as a service & dark data assessments – powered by Veritas
- ✓ Risk register automation – powered by Calqrisk
- ✓ Penetration testing & vulnerability assessments
- ✓ Data classification and labelling
- ✓ Microsoft 365 security & compliance current state assessment
- ✓ Business continuity & resiliency planning before the event
- ✓ Disaster recovery point and time (RPO, RTO) validation testing

PROTECT

This function is focused on ensuring safeguards are in place to enable the continued delivery of infrastructure and data services. bluesource can assist through the design and implementation of information management & protection, data loss prevention techniques, advanced threat protection, identity management & protection, and device management & protection.

Products, partners and solution areas

- ✓ Identity access management & protection – powered by Microsoft Azure Active
- ✓ Directory conditional access, multi-factor authentication & privileged ID management
- ✓ Data access control – powered by Torsion
- ✓ Data management and protection – powered by Microsoft Information Protection
- ✓ Data loss prevention – powered by Microsoft, Netskope & Mimecast
- ✓ Device management and protection – powered by Microsoft Endpoint Manager
- ✓ Next generation endpoint security – powered by CrowdStrike and Microsoft Defender for Endpoint
- ✓ bluesource backup-as-a-service delivering immutable and indelible back-ups – powered – powered by Veritas, Rubrik
- ✓ Email security – powered by Mimecast & Microsoft
- ✓ Secure Access Service Edge framework network security including - Secure Web Gateway, Cloud Access Security Brokerage and Zero Trust Network Access – powered by Netskope
- ✓ Data Erasure on obsolete equipment – powered by Blancco
- ✓ Employee security awareness training – powered by Mimecast
- ✓ bluesource managed updates for operating systems, Exchange, SharePoint, Enterprise Vault and Azure Virtual Desktop

Copyright © 2021
All rights reserved

DETECT

Detect services are focussed around the identification of anomalous or malicious activities by bad actors, insider threats and potential breaches.

Products, partners and solution areas

- ✓ Cloud security posture management – powered by Netskope & Microsoft
- ✓ Cloud access security brokerage – powered by Netskope & Microsoft
- ✓ Discovery of sensitive data in areas that are not appropriately protected – powered by Veritas & Microsoft
- ✓ Endpoint Detect & Respond – powered by CrowdStrike & Microsoft
- ✓ Behavioural analytics to identify unusual activities such as mass copies, deletions and logins – powered by Microsoft & Netskope
- ✓ Detection and prediction of Insider Threats by learning regular patterns of activity for each insider
- ✓ bluesource MDR – powered by CrowdStrike, Mimecast & ECSC Back up healthchecks – Most companies are not adhering to industry best practices for backing up data. We can offer some expertise in this area

RESPOND

These services focus around having appropriate solutions, services and processes in place to help contain a breach and know when and how to invoke a recovery. Advanced threat protection services can ensure that detected threats are remediated across all platforms simultaneously to eradicate malware from all in-scope services.

Products, partners and solution areas

- ✓ Incident response retainer – powered by ECSC
- ✓ Incident response consultancy to assist with managing an active incident – powered by ECSC
- ✓ Implementing recommended remediations – powered by bluesource professional services

RECOVER

This function is focussed on the restoration and remediation of services following an attack. bluesource can assist via our Backup as a Service (BaaS) offering along with our professional services team who can assist with the rebuilding of your infrastructure.

Products, partners and solution areas

- ✓ Disaster recovery plan execution – powered by Azure, Zerto & Rubrik
- ✓ Bare metal restores
- ✓ SaaS data restores
- ✓ System rebuilds
- ✓ Ontrack recovery – If the worst comes to the worst and you do end up with encrypted production and backup systems we can take a sample of the encrypted code and using a range of Ontrack recovery services we can potentially recover data that has been encrypted

Protect your data from Ransomware attacks by starting a conversation with us today.

bluesource
Protect
Govern
Move
Manage

0345 319 2300
hello@bluesource.co.uk
www.bluesource.co.uk

bluesource
122 Tooley Street,
London, SE1 2TU