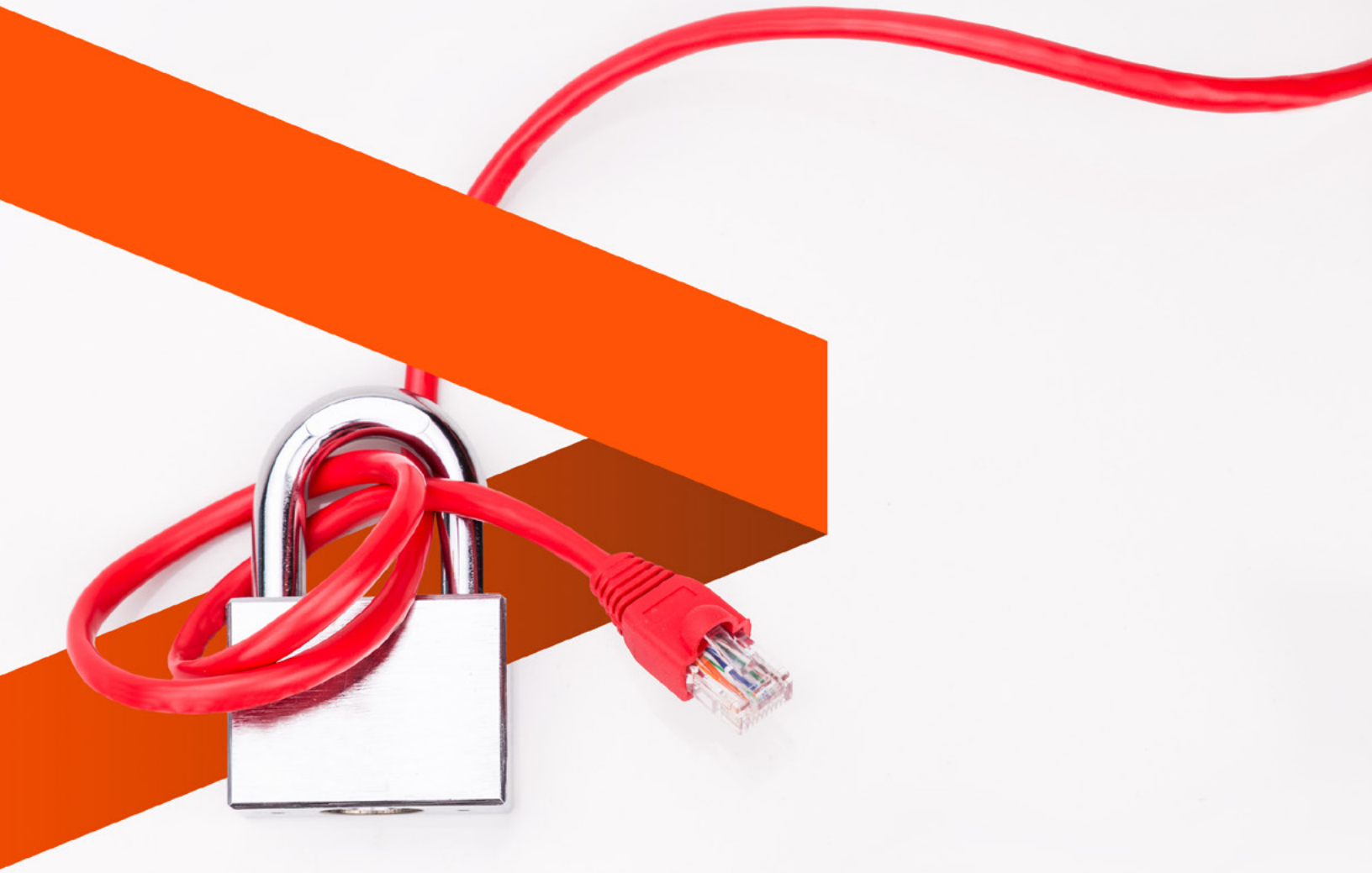


MANAGING RANSOMWARE

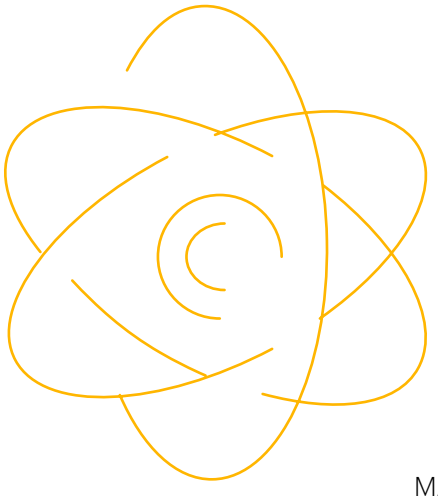
PRACTICAL STEPS TO AVOID FUTURE ATTACKS

Accenture Security

The iDefense Threat Intelligence team of Accenture Security highlighted a new dynamic in its cyber crime analysis: ransomware-as-a-service (RaaS). Malicious actors packaged successful variants of extortive malware into kits that could enable less-skilled malicious actors to employ this threat tactic with little effort or technical knowledge. It is a new take on an age-old problem that is making the C-suite increasingly nervous.

Asking for a ransom as a means of coercion can be traced back thousands of years. As its latest incarnation, ransomware introduces malicious software onto a target computer or server to exploit one or more programmatic flaws and gain expanded access to the computer. A few encryption technologies later, with files "locked" with an encryption key that only the attacker possesses, the impacted user is asked to pay money—often in the digital currency bitcoin—to reinstate access to the encrypted files.

Ransomware in itself is not the real risk. The risk lies in the impact to the business that is caused by a service or process that has been suddenly removed. Ransomware can halt manufacturing control systems, potentially shutting down plants, or ransomware can target a bank's clearing systems and cause a backlog in the clearing process. In the first half of 2016, there were widespread reports on the Internet of new ransomware variants and infections affecting various organizations across a wide swath of industries in both the public and private sectors. One well-publicized report concerned the Hollywood Presbyterian Medical Center ransomware infection in February 2016. In addition to turning away ambulances, hospital staff were forced to manually write down patient information because they had no access to computers, and eventually, the hospital declared an internal state of emergency.



Fast forward to 2017, and the cyber attack scenario was repeated across the National Health Service in the United Kingdom and many other organizations globally. Ransomware is not new, but the size of recent attacks such as WannaCry and Petya is "unprecedented," according to European Union police body Europol.

Although the technical debriefs following such incidents give vital information about what has happened, corporate executives and Board members are often left wondering how to understand the real risk associated with ransomware and, more important, how to identify the best steps to manage or mitigate such exposure. In reality, ransomware could have a profound effect on profitability, reputation and shareholder value. C-suite executives should strive to better understand the range and depth of their digital agenda to be able to characterize the complex risks presented by these cyber threats.

Without doubt, ransomware is growing in the extent of its boldness and veracity. Future outbreaks are likely to be faster and stronger, and attempt to inflict more damage to their targets. But technically and tactically, there are a range of activities that, together, will help defend and respond more effectively to ransomware outbreaks. From a Board and C-suite perspective, understanding their organization's most critical products, services, business processes and data is crucial. Protection and end user education are similarly vital. And being able to respond quickly in an ongoing way, can also help any defense and response approach. Fortunately, there are a number of tactical steps that can be taken to avoid falling victim to a ransomware attack. Read on to find out more about the necessary practices that leading companies are taking to protect themselves.

E-MAIL **ATTACKS**

Many ransomware attacks, with WannaCry and Petya being notable exceptions, originate as a malicious e-mail. Prevention training and awareness programs can help employees recognize telltale signs of malicious e-mails and phishing scams and how to handle them. **Leading programs typically include:**

Training to help employees recognize and avoid fraudulent e-mails.

Guidance on how to respond if an employee believes he or she is victim of a social engineering attack.

Frequent tests that assess employees' adoption of the guidance provided.

RANSOMWARE AND E-MAIL **CONTROLS**

Ransomware attacks are frequently delivered via e-mail. Strengthening e-mail controls can often prevent malicious e-mails from reaching employees. **Consider taking the following steps to protect e-mail environments:**

- Enable strong spam filters to prevent suspicious e-mails from reaching end users.
- Authenticate inbound e-mail using Sender Policy Framework and Domain Keys Identified Mail to prevent spoofing.
- Scan incoming and outgoing e-mails to detect threats and filter executable files.
- Deploy a cloud-based e-mail analytics solution such as Proofpoint or Microsoft ATP to identify and quarantine known threats distributed via malicious e-mail.
- Configure e-mail in a manner that clearly identifies external e-mail as originating from outside the enterprise, prompting employees to be more cautious.
- Display file extensions, making it is easier to spot file types not commonly sent to employees, such as JavaScript.
- Consider installing the Microsoft Office viewers that do not support macros to enable employees to see document content without opening the document.

PROTECTING INFRASTRUCTURE

Attackers are getting smarter and unsuspecting employees can make mistakes and fail to recognize malicious e-mails. In these cases, the following actions could be considered to help protect your infrastructure:

Remove or limit local workstation admin rights, as well as closely monitor privileged administrator access across operating systems (Windows Domain Admin accounts, UNIX root accounts) in SIEM.

Use endpoint protection that includes heuristic behavior analysis and updates signatures frequently. Institute a monitoring program to track endpoints that have not received these updates on a regular basis.

Maintain a workstation security compliance program to validate that all relevant tools are in place and working. This includes content within SIEM platforms to monitor for new, updated or removed controls.

Segment networks so servers and workstations are not in the same network. Place strong access control lists between these networks.

Review security systems for appropriate configurations/hardening (virus scanners, firewalls, intrusion prevention systems, e-mail/Web gateways).

Set default execution commands to "no." This helps keep servers secure by identifying authorized applications and limiting what each can change and update. It also prevents attempts to make changes that block ransomware from contacting command and control servers and downloading malicious software.

Regularly patch operating systems and applications so that known vulnerabilities are not exploited. Track individual employee and server assets to ensure compliance across the enterprise. It only takes one endpoint to infect others.

Limit administrator access to only those "in need."

Configure security, information and event management (SIEM) solutions to flag incidents and enable automated cleanup methods.

Implement and/or tighten web filters/URL blockers. Along with clicking on links within phishing e-mails, employees introduce malware by visiting compromised webpages. Web filtering helps block websites hosting ransomware, as well as their command and control servers.

Deploy a cloud-based threat reputation tool such as OpenDNS, Forcepoint or Palo Alto that blocks traffic from known malicious websites.

A STRONG BUSINESS **CONTINUITY PLAN**

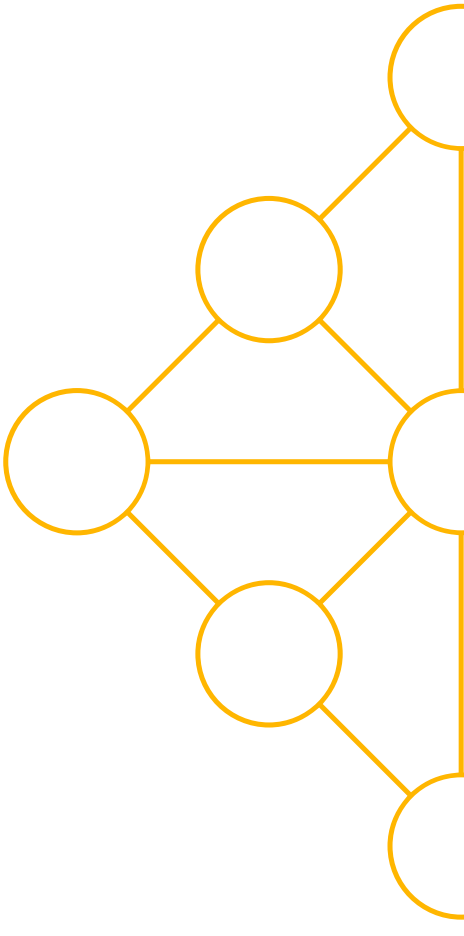
Ransomware attacks are not random but rather targeted and intentional. Organizations should prepare and exercise a crisis management plan well in advance of an incident. This includes emergency shutdown procedures and instructions for employee communication, "out-of-band" communications (voice systems may be down during a cyber attack) as well as having legal and PR teams educated on these responses.

Even with the best defenses in place, successful attacks may still occur. Having a strong business continuity plan for recovery could make it easier to avoid paying ransom. **Key components for a business continuity plan to be effective against ransomware include:**

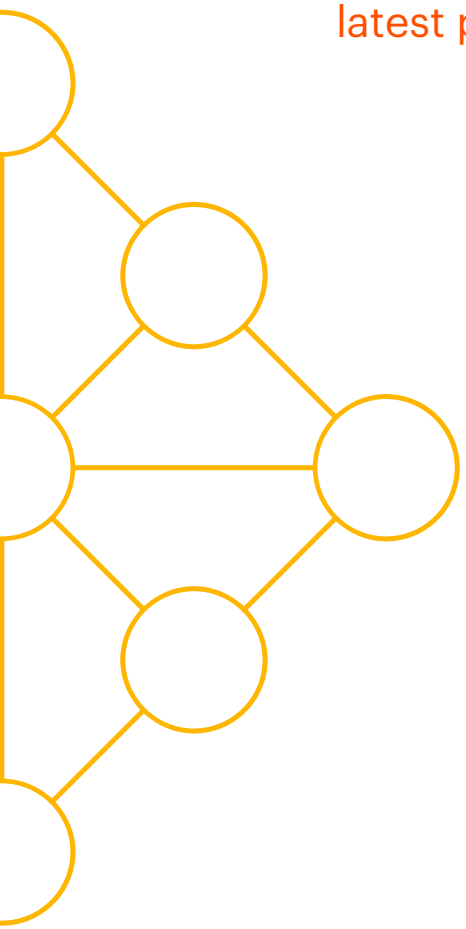
Alignment of recovery objectives to the critical tasks within an acceptable timeframe.

A regular review, update and test of the recovery plan.

Workstations and file servers should not be constantly connected to their backup devices (so that in the event of a successful attack, backups will not be encrypted). In addition, confirm that your backup solution stores periodic snapshots instead of regular overwrites of previous backups.



Accenture recommends that all organizations review their current processes against these leading practices and close any gaps. And while these recommendations can reduce an organization's vulnerability to ransomware attacks, they may not be fully sufficient as the threat evolves. So we also urge organizations to stay informed about emerging threats and the latest practices required to avoid those threats.



Find out more about the evolving cybersecurity landscape and what you can do to strengthen your defenses.

CONTACT

Justin Harvey
Managing Director, Accenture Security
Incident Response & Threat Hunting
justin.harvey@accenture.com

Josh Ray
Managing Director, Accenture Security
Cyber Threat Intelligence
joshua.a.ray@accenture.com

Uwe Kissmann
Managing Director, Accenture Security
uwe.kissmann@accenture.com

Rick Hemsley
Managing Director, Accenture Security
rick.hemsley@accenture.com

Gareth Russell
Manging Director, Accenture Security
gareth.russell@accenture.com

Visit us at http://www.accenture.com/security

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.