“Automatic Repair” of Hacked Web Sites - an Information Security “Best Practice”

A White Paper by

Lockstep Systems, Inc.
+1-480-596-9432
1-877-WEB-FIXR

info@lockstep.com

www.lockstep.com

"Automatic Repair" of Hacked Web Sites -- an Information Security "Best Practice"

A White Paper by Lockstep Systems, Inc.

Introduction

Your web site is crucial to your business. What happens if it goes down? What happens when a hacker paints a political slogan on your home page, or steals your customer's credit card information? Will your firewall keep you safe? Will your intrusion detection tools catch everything?

No. Unfortunately, widely used "detect and prevent" methods don't always keep the bad guys out of a web site. You need an automatic way to fix your web site when the bad guys do get through.

"Automatic Repair" technology from Lockstep Systems automatically restores the correct content to your web site if a hacker has changes something. Our WebAgain software is the first on the market to provide "Automatic Repair" for web site content. Now companies can confidently employ "Automatic Repair" as a "Best Practice."

Web Site Content Dependence and Risks

Reliable, always-available web sites are increasingly crucial to business and government enterprises. The integrity of content (e.g. web pages, images and scripts) comprising such web sites must be preserved to ensure availability and reliability.

Because of their dependence on their web sites, enterprises face considerable risks if web site content integrity is compromised or content is altered by unauthorized means:

- ***Business Disruption***
  Web site downtime due to corrupted content can be measured in terms of lost opportunity and the cost of alternative manual methods. For example, a $100 million/year e-business could lose over $10,000 of revenue per hour of downtime if orders cannot be processed. Manual transactions, which may be necessary to replace the online order process while a web site is unavailable, are typically far more costly than on-line transactions.

- ***Cost to Recover***
  Recovery from content corruption can be costly if the recovery is based on reactive, manual methods. In a typical web site corruption incident, after a hack has been reported by a customer or employee, the web site is taken off line, a correct backup is located, and the web site is restored manually, usually in a panic mode. Money, time and frustration can be saved if the recovery is proactive and automatic, not reactive and manual.

LOCKSTEP®

- ***Public Image***
  A web site is a crucial element of an enterprise's public relations and customer interaction strategy. A home page defaced with pornography or political propaganda can be irritating or insulting to customers or constituents, thereby undermining confidence in the enterprise.

- ***Transaction Theft.***
  While the majority of web site content corruption is the result of vandalism (electronic graffiti), a recent survey stated that fully 13% of respondents whose web sites had been hacked had experienced the theft of transaction information as a direct result of the intrusion. [i] This can occur when a hacker changes a script or program on the web site to divert sensitive customer information (e.g. credit card number or confidential details) to illicit destinations.

- ***Legal Liability***
  If legally-binding documents (e.g. privacy policies, price lists, terms and conditions, financial results) are modified by a hacker and other web site visitors innocently rely on the altered content to make business decisions, the enterprise may incur unforeseen and potentially costly legal liability.

Hacking Threat

Enterprises are increasingly subject to these risks because of the geometrically escalating threat of web site content corruption by hackers. In an increasingly hostile global Internet environment, computer system intrusions are more than doubling each year [ii] because hackers are employing sophisticated automation tools and becoming much more focused in their attacks. [iii]

Eileen Colkin recently reported, "Cyberattack activity increased 79% between July and December last year [2001], according to a survey of 300 businesses released last week by security services vendor Riptech, Inc. The survey analyzed attacks by geography and company type and said most attacks were launched from China, South Korea, and the US. Power and energy companies suffered severe attacks at almost twice the rate of other industries." [iv] Riptech's analysis of targeted versus opportunistic attacks further suggests that 39% of attacks were targeted toward a specific organization, while 61% were opportunistic in nature. [v]

A report on the current state of computer crime and information security published in 2001 by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) revealed that 23% of survey respondents reported that their web sites had been hacked (another 27% didn't know), and over half of those had their web sites hacked ten or more times. 90% of the web site hacks were just vandalism, but 13% included theft of transaction information. [vi]

Bruce Schneier, CTO of Counterpane, commenting on the CSI/FBI study, remarked, "The financial consequences are scary. Only 196 respondents would quantify their losses, which totaled $378M. From under 200 companies! In one year! This is a big deal … the trends are unnerving. It's clearly a dangerous world, and has been for years. It's not getting better, even given the widespread deployment of computer security technologies. And it's costing American businesses billions, easily." [vii]

LOCKSTEP®

Gartner estimated that half of all small-midsize enterprises will suffer an Internet attack by 2003, and that "more than 60% of companies that are targeted will be unaware of the attacks." [viii] The estimated percentages forecast by Gartner may seem terribly high, unless one considers that, according to the CSI/FBI study, we are already half way there.

The Riptech report, based on detailed empirical analysis of actual attack statistics, indicates that the Gartner prediction may have been conservative: "The scope of attack activity over the past six months was extremely broad. In fact, 100% of the sample experienced some form of attack activity. This discovery strongly indicates that the extent of the threat on the Internet may be even greater than indicated by several recent reports. In fact, our findings strongly suggest that once companies connect their systems to the Internet, they are virtually guaranteed to suffer some form of attack activity. … critical and emergency-level events have been detected on the networks of 43% of Riptech's clients, indicating that, without real-time intervention, actual security breaches were imminent at some point in the past six months for nearly half of Riptech's clients." [ix]

Riptech concludes its report with this admonition, "…the Internet security threat is real, pervasive, and perhaps more severe than previously anticipated. Stakeholders of Internet-connected organizations should ensure that appropriate measures have been taken to address this increasing threat rate." [x]

In response to these current threatening industry conditions, Charles Kology, IDC security analyst, asserted, "The bottom line is that security is now a mandatory consideration, not just a discretionary purchase." [xi]

Current Best Practices are Insufficient

Despite widespread implementation of information security best practices to counteract the hacking threat, systems are still vulnerable to attack. Current "best practices" are insufficient to deal with the increasing aggression and automation of hackers.

Current best practices in information security (including both technology and processes) may be divided into two major categories:

- ***Intrusion Prevention***
  Technologies such as firewalls, encryption, user authentication/authorization and virus protection are widely deployed to prevent unwanted intrusions. Additionally, correctly configuring operating systems and applications and applying the latest software updates from vendors is highly recommended (but less widely practiced).

- ***Intrusion Detection***
  Recognizing that intrusion prevention methods are subject to compromise, many enterprises employ intrusion detection methods to identify when hackers are attacking their systems. Alerted to intrusions in progress, system operators can take manual action to thwart hackers.

In spite of the best efforts to protect information systems in general and web sites in particular, experience and theory both show that increasingly complex and interconnected information systems cannot be completely protected.

LOCKSTEP®

A recent technical report published by Carnegie Mellon's Software Engineering Institute (SEI) stated, "Despite the best efforts of security practitioners, no amount of system hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack." [xii]

BBN researchers exploring Intrusion Tolerant Systems, have written, "The approach taken by traditional security engineering attempts to protect the infrastructure resources from intruders by establishing a preventive barrier. … For instance, firewalls, a network layer barrier, do not normally interact with applications that use the network. Similarly, IDSs (Intrusion Detection Systems) operating at various system layers hardly ever cooperate among themselves or interact with other kinds of applications. While the world is gravitating towards more use of COTS (commercial-off-the-shelf) components and more integration of diverse and distributed resources, security mechanisms attempting to prevent attacks are bound to be imperfect. … even the 'defense in depth' approach cannot guarantee that critical systems will be completely shielded from the attackers." [xiii]

Even in the face of such expert counsel, many organizations feel a false sense of safety if a firewall is in place. Particularly in the case of public web servers, the very fact that a firewall must provide an open door through which content is served makes the web server vulnerable to attack. Riptech concludes: "By design, public web servers respond to requests from remote systems on the Internet. Any flaw in processing these requests can result in the emergence of a high-risk vulnerability virtually overnight. Code Red is a perfect example of this. Firewalls are largely ineffective against this type of threat because most operate on a simple model of allow/deny. Therefore, if the firewall is configured to allow web connections to a web server, the firewall will also allow web attacks to the same server. Some content-filtering proxies and firewalls are designed to address this problem, but these systems negatively impact performance and are far from 100% effective." [xiv]

Drawing conclusions from the CSI/FBI survey, Bruce Schneier stated, "What's interesting is that all of these attacks occurred despite the wide deployment of security technologies: 95% have firewalls, 61% an IDS (Intrusion Detection System), 90% access control of some sort, 42% digital IDs, etc. Clearly the technologies are not working sufficiently well." [xv]

Automatic Repair as a Best Practice

So, what does one do to find relative stability in this hostile environment? Perhaps the answer lies in a simple analogy. A jewelry store owner may attempt to protect his valuable merchandise from thieves by employing good preventative measures - (e.g. locks, shatterproof glass display cases, trustworthy employees) and good intrusion detection methods (e.g. window alarms, motion detectors, automatic calls to police) but still buys good theft insurance - for the unwanted, but still potential, case where an innovative thief breaks through the defenses, thwarts the detection methods and still steals the diamonds. The insurance is a means of recovering after business has been disrupted by theft.

Similarly "Automatic Repair," analogous to the store's theft insurance, is emerging as an information security "Best Practice" for enterprises that may already employ Intrusion Prevention measures (e.g. firewalls, encryption, user authentication) and Intrusion Detection systems (IDS), but recognize that hackers may still get through and corrupt their systems. It is a means for a company to easily recover from, or to survive the effects of, an illicit intrusion.

LOCKSTEP®

In commenting on groundbreaking system survivability research at SEI, Jeannette M. Wing, of Carnegie Mellon University stated, "Survivability is the ability of a system to continue operating despite the presence of abnormal events such as accidental failures and malicious intrusions. Ensuring system survivability has increased in importance as critical infrastructures have become heavily dependent on computers." [xvi]

A recent SEI report stated, "The discipline of survivability can help ensure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions." [xvii]

In introducing their Intrusion Tolerant Systems work, BBN Technologies researchers stated, "We argue that development and support of intrusion-aware survivable applications, i.e., applications that react to intrusions and survive their consequences, are key problems in the area of intrusion tolerant systems." [xviii]

As research progresses in the broad areas of system survivability and intrusion tolerance, commercially-available "Automatic Repair" products are emerging in select areas to contribute to overall system survivability. Such automatic repair products should be deployed as best practices" to augment Intrusion Prevention and Intrusion Detection best practices.

The best-known example of automatic repair technology is virus protection software. Not only do widely-deployed commercial virus protection products automatically detect the presence of unwanted software viruses or worms, they can automatically remove the offending files, thereby enabling the system to survive the viral attack.

The WebAgain software product from Lockstep Systems, Inc. takes the next step forward toward system survivability. It is the first commercially available product to provide automatic repair for hacked web site content. Using a patent-pending process, the WebAgain product automatically repairs the content of hacked web sites by automatically detecting unauthorized changes to web site content and automatically restoring the original content, all without human intervention. [xix]

By addressing an important and timely, but well-understood and clearly bounded application area, Lockstep is able to provide a commercially-available and easily deployed survivable system solution for automatically detecting content corruption and automatically restoring the correct content to a hacked site.

LOCKSTEP®

Deployment of the WebAgain product as an information security best practice can help enterprises minimize the risks of web site content corruption:

- ***Business Disruption***
  Web site downtime will be minimized because correct content will be automatically and quickly restored if a hack occurs.

- ***Cost to Recover***
  Because recovery from content corruption is automatic and rapid, rather than manual and panic-stricken, recovery costs will be insignificant.

- ***Public Image***
  Because offending material is immediately removed, customers and constituents will not lose confidence in the enterprise.

- ***Transaction Theft***
  Because both visual pages and hidden scripts are both protected, a hacker's attempt to corrupt the transaction flow by altering scripts will be quickly repaired.

- ***Legal Liability***
  Because legally-binding information will remain what it should be, the risk of legal liability due to changed content is minimized.

Conclusion

Enterprises that depend on reliable, available web sites face significant operational risks because of the geometrically escalating threat of content corruption, despite Intrusion Prevention and Intrusion Detection methods being widely deployed as information security best practices. As research progresses in the areas of system survivability and intrusion tolerance, "Automatic Repair" is emerging as an information security best practice to further protect enterprises from the effects of hacking. By providing Automatic Repair of web site hacks, the WebAgain software product from Lockstep Systems, Inc., can help enterprises minimize the significant business risks caused by the threat of web site hacks as they deploy "Automatic Repair" as a best practice survivable system solution.

LOCKSTEP®

[i] 2001 Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey

[ii] Computer Emergency Response Team

[iii] Don Clarke, Hackers Turned to Specific Companies As Attacks Accelerated in Late 2001, Wall Street Journal, January 28, 2002

[iv] Eileen Colkin, Information Week, Top of The Week News Scan, February 4, 2002

[v] Riptech Internet Security Threat Report, January 2002, p. 13.

[vi] 2001 Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey

[vii] Bruce Schneier, Cryptogram, April 15, 2001

[viii] IDG News Service, October 10, 2000

[ix] Riptech Internet Security Threat Report, January 2002, p. 15.

[x] Riptech Internet Security Threat Report, January 2002, p. 24

[xi] IDC Opinion: September 11 Implications for Security Markets

[xii] Survivable Network Systems: An Emerging Discipline, Technical Report Carnegie Mellon, Software Engineering Institute

[xiii] Intrusion Tolerant Systems, Partha P. Pal, Franklin Webber, Richard E. Schantz and Joseph P. Loyall, BBN Technologies

[xiv] Riptech Internet Security Threat Report, January 2002, p. B-6

[xv] Bruce Schneier, Cryptogram, April 15, 2001 (commenting on the CSI/FBI survey)

[xvi] Jeannette M. Wing, Carnegie Mellon University, Cornell Department of Computer Science Colloquium, October 4, 2001

[xvii] Survivable Network Systems: An Emerging Discipline, Technical Report Carnegie Mellon, Software Engineering Institute

[xviii] Intrusion Tolerant Systems, Partha P. Pal, Franklin Webber, Richard E. Schantz and Joseph P. Loyall, BBN Technologies

[xix] WebAgain product information: http://www.lockstep.com/products/webagain/wa-product.html

LOCKSTEP®