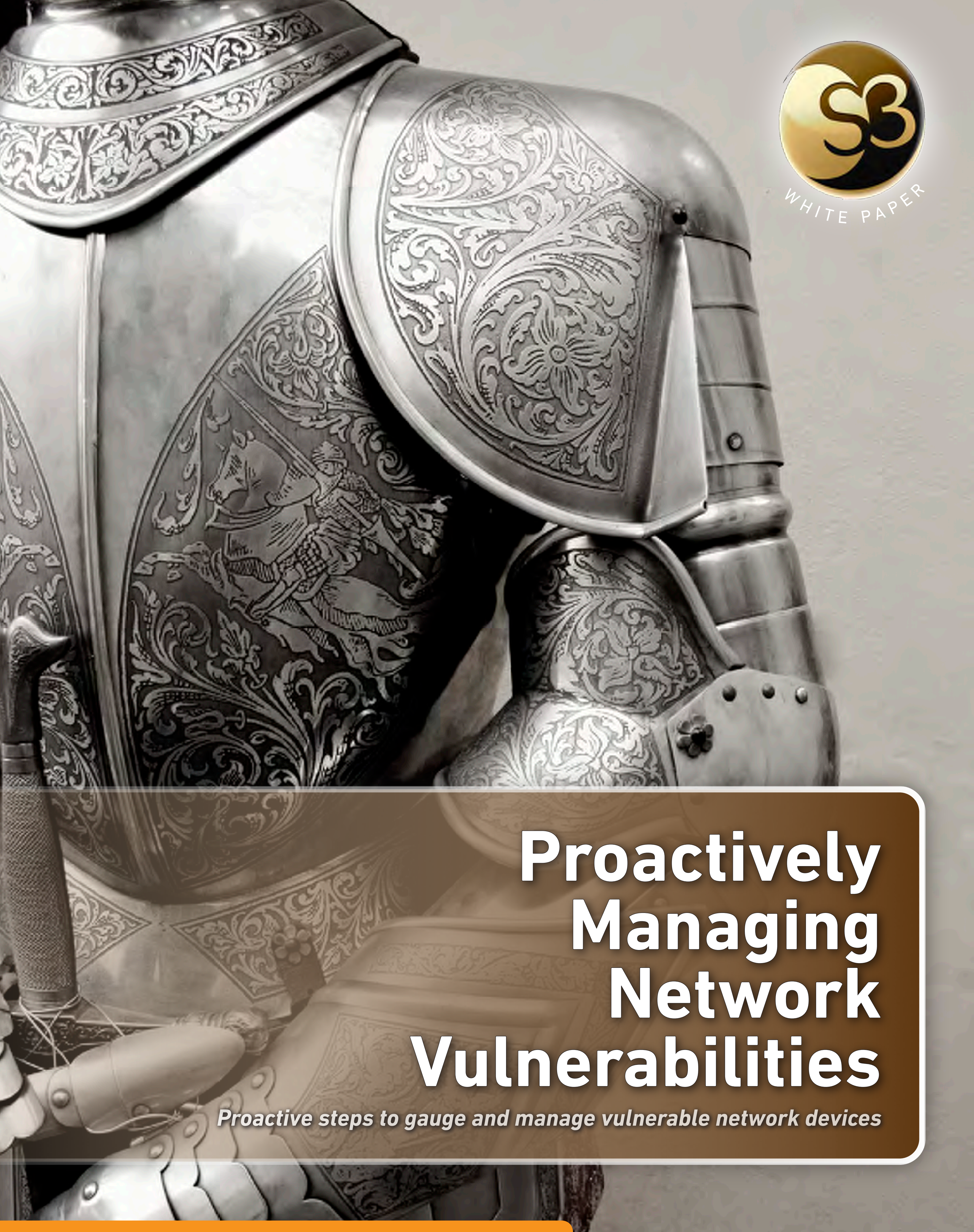


WHITE PAPER

Proactively Managing Network Vulnerabilities

Proactive steps to gauge and manage vulnerable network devices

overview

The more data the better. This is true of any predictive calculation. That's why S3's Canary™ strives to provide a device's realized MTBF by using the combined service ticket data of many enterprises. The realized MTBF is then merged with customizable criticality rules to provide a predicted date of device failure, and an impact assessment if a device goes down.

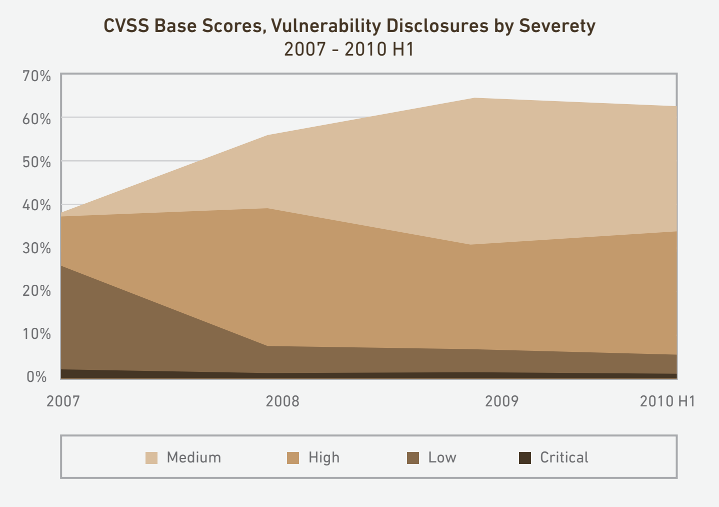
To get to there, Canary™ starts with vulnerability management. What is out there right now that can bring the network to its knees? What's the best way to mitigate those risks? Does everything need to be patched? What's the impact of an exploited vulnerability? Answering those questions is the first step to upgrading a NOC from reactive to proactive. That's where Canary™ begins.

contents

introduction

INDUSTRY	APPLICATION	AVERAGE COST PER HOUR OF DOWNTIME (US$)
Financial	Brokerage operations	$7,840,000
Financial	Credit card sales	$3,160,000
Media	Pay-per-view	$183,000
Retail	Home shopping (TV)	$137,000
Retail	Catalog sales	$109,000
Transportation	Airline reservations	$108,000
Entertainment	Tele-ticket sales	$83,000
Shipping	Package shipping	$34,000
Financial	ATM fees	$18,000

Source: Contingency Planning Research



Source: IBM X-Force(r) 2010 Mid-Year Trend and Risk Report

Corporate global networks are growing drastically through acquisitions and organically. Often, the growth occurs too quickly to mitigate risk through reactive, infrequent vulnerability assessments, testing and deployments. Should vulnerabilities on a network not be managed appropriately, the impact of the resulting downtime could cost a company as much as $7.8 million per hour[1].

Some IT organizations rely on equipment vendors for vulnerability assessments. However, many vendors will not announce vulnerabilities until proven patches are available[2], and assessments are not performed frequently enough to catch new vulnerabilities in time.

Other IT organizations manually compare vulnerability announcements to network scans and perform their own assessments. However, this method is becoming more complicated and time consuming with the number of vulnerabilities expected to double in 2010 compared to 2009[3]. The criticality of the vulnerabilities isn't helping matters, either. The number of high-severity vulnerabilities has increased by 33% since 2008[4].

Vulnerability notification services exist today that provide a centralized source for vulnerabilities reported by equipment vendors. These products, however, fail to provide information on how these vulnerabilities impact the organization's productivity and revenue.

[1] *Contingency Planning Research – division of Eagle Rock Alliance, Ltd. http://www.eaglerockalliance.com.*

[2] *Peter Mell, Tiffany Bergeron, David Henning, "Recommendations of the National Institute of Standards and Technology (NIST)", 1November 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf*

[3] *"Number of Vulnerabilities Expected to Double this Year" – by Lucian Constantin. July 12th, 2010. http://news.softpedia.com/news/Number-of-Vulnerabilities-Expected-to-Double-this-Year-147186.shtml*

[4] *"IBM Security X-Force® 2010 Mid-Year Trend and Risk Report", IBM. August 2010. http://www-935.ibm.com/services/us/iss/xforce/trendreports/*

introduction

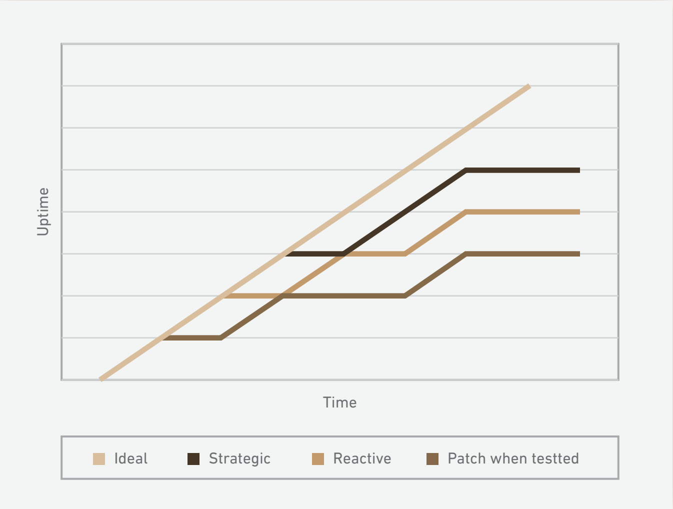
> “THE PRIMARY GOAL OF ANY NOC IS TO PROACTIVELY MANAGE DEVICES TO REDUCE DOWNTIME”

Without a business-centric, prioritized view, Network Operations Centers (NOCs) are inundated by thousands of change requests. Most of those do not have any real effect on the reliability of the network.

Once vulnerabilities are identified, the NOC has the daunting task of configuring and testing patches developed to fix the problem. The severity of some vulnerabilities often requires detailed testing to be put on hold until after deployment. With multiple levels of testing and several vulnerabilities in a network, tracking the testing of the vulnerabilities must be done to ensure nothing is missed.

There are even multiple deployment methods to consider, each of which could impact the amount of downtime incurred and overall vulnerability exposure. The recommended strategic deployment method, which balances risk and downtime, requires bundling, scheduling, and tracking of deployments.

Source: Solaris Patch Management: Recommended Strategy



The recommended strategic deployment method, which balances risk and downtime, requires handling, scheduling and tracking of deployments.

Automation of vulnerability detection, prioritization, and management of testing and deployment is a proactive, cost-effective way to perform business-directed vulnerability management.

This paper provides steps an organization should follow to establish processes, and it describes tools to address various network vulnerabilities.

In the end, the primary goal of any NOC is to proactively manage devices to reduce downtime and fire fighting. By providing prioritized alerts on vulnerabilities and the realized Mean Time Between Failures (MTBFs) of devices, the S3® Canary™ system helps achieve that goal.

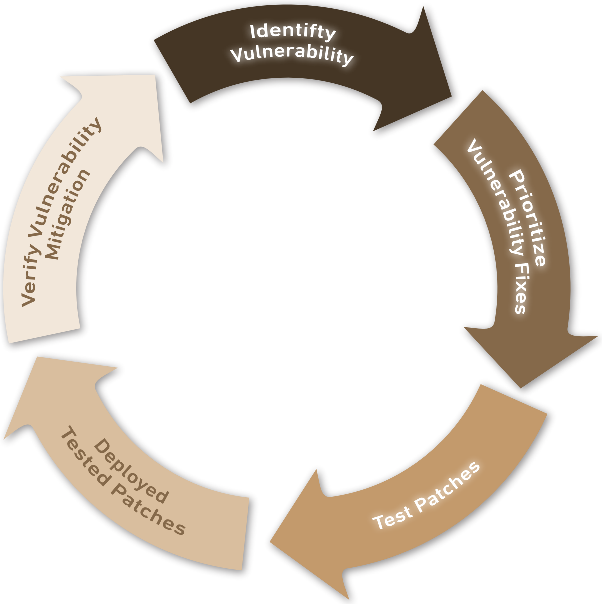
establishing a vulnerability management process

The vulnerability management group for any NOC has 5 primary functions:

- Identify vulnerabilities.
- Prioritize patches.
- Obtain & test patches.
- Deploy patches.
- Verify vulnerability mitigation.

The absence of one of these functions could cause network downtime or security breaches.

Every NOC should have established guidelines and tools to assist with each function. The goals of each step and common approaches are described below.


Identifty Vulnerability
Prioritize Vulnerability Fixes
Test Patches
Deployed Tested Patches
Verify Vulnerability Mitigation

IDENTIFICATION OF VULNERABILITIES

In order to mitigate vulnerabilities, they must be identified. Depending on the network vendors, there may be multiple sources for this information. Some of the most common methodologies for identifying vulnerabilities as well as the strengths and weaknesses of each are described below.

NOCs tend to use one of the following methods to identify vulnerabilities:

- Equipment vendor or 3rd network assessments (where consultants scan the network and identify vulnerabilities).
  >> Benefits:
  - » Can be purchased and performed as needed or as budgets allow.
  - » Knowledgeable sources (typically trusted partners of equipment manufacturers) perform the assessments and offer valuable insight to network performance/security.

  >> Consequences:
  - » Vulnerability information is only a snapshot and up-to-date visibility of vulnerabilities can only be achieved by purchasing another network assessment.
  - » Vulnerabilities without patches or resolutions may not come up during the assessment.
  - » If the vendor is a trusted partner of an equipment manufacturer, they may only provide assessments on those pieces of equipment.

- Manually gathering published vulnerability information and comparing it to other data sources. Sources can include a NOC-maintained CMDB, network scans, IMAC/MACD systems, or TEMS systems.
  >> Benefits:
  - » Completely controlled by in-house staff. Allows for customization of management processes.

- >> Consequences:
  - » Time consuming.
  - » Some manufacturers do not publish vulnerability information until a patch or workaround is available.

- Subscribing to a vulnerability identification service such as Secunia's EVM, Symantec's Deepsight or S3's Canary™. These services allow customers to see up-to-date vulnerabilities as it applies to their network scans. Some services even offer the application of customized business-directed prioritization rules against the results so that the most potentially damaging vulnerabilities can be handled first.
  - >> Benefits:
    - » Pulls vulnerabilities from several sources.
    - » Provides insight to the severity of the vulnerabilities and often provides suggested resolutions.
    - » Automatically identifies equipment from the organization's network scans that have the vulnerabilities.
  - >> Consequences:
    - » No vulnerability is excluded, so the results may inundate the NOC. This is true of most vulnerability identification services. The exception is S3's Canary™ which allows the NOC to identify critical assets, sites and applications to prioritize issues in their order of importance to the network and enterprise.

Once vulnerabilities have been identified, those critical applications affecting business applications or locations should be resolved first, ensuring that valuable IT time is spent most effectively.

PRIORITIZATION OF VULNERABILITY FIXES

In order to support addressing the most critical vulnerabilities first, the results of the identification process must be verified then prioritized.

The initial identification results in some false positives regardless of the identification method used. Examples of false positive results or misleading vulnerabilities include:

- Devices that have the vulnerable software IOS, but don't utilize the protocol or function that is impacted.
- Devices in a network-test environment that are being utilized by the network management team to test vulnerability fixes.

The NOC must verify the identification results and remove any invalid or misleading vulnerabilities. Even with those removed; there will still be thousands of identified vulnerabilities to review. Without prioritization, this is a nightmarish, manual job, which NOCs won't have time to complete – leaving the network at risk.

Understanding the revenue and productivity impact of vulnerabilities is the key to prioritizing review, patch testing and deployment. However, using just the impacted headcount and estimated lost revenue isn't enough to get a good picture. Any downtime calculation must take into account the potential lost sales, damaged reputation, and even compliance laws.

establishing a vulnerability management process

As an example, in 2007, Minnesota established the "Plastic Card Security Act," which states that any company that is breached and found to have been storing "prohibited" credit card data is required to reimburse banks and other entities for costs associated with blocking and reissuing cards. This law also opens up these companies to private lawsuits.[5]

NOCs typically use one of the following methods to prioritize vulnerabilities:

- Downtime impact calculators. These utilize specific business inputs to determine the true cost of network downtime. The most prevalent calculator is the one created in conjunction with Warwick Business School and Networks First .[6]
  - >> Benefits
    - » Allows calculations to be precise by quantifying restoration time, potential lost sales and damaged reputation in addition to revenue and productivity impacts.
  - >> Consequences
    - » Requires significant amount of data inputs.
    - » Calculation complexity can lead to a paralysis by analysis scenario when prioritized vulnerabilities do not align as expected.
    - » Industry-specific rules (such as taking into account compliance laws) become lost in the data.

- Application prioritization. The fastest way to prioritize vulnerability fixes is to apply criticalities to the applications that run over the devices. S3's Canary™ product allows users to specify criticality by application, site and asset.
  - >> Benefits
    - » Keeps revenue flowing through the business. For example, if a router goes down that prohibits 20 users from accessing SAP, is that a highly critical event?
    - » Intuitive inputs that don't require a large amount of data.
  - >> Consequences
    - » Is not as precise as using a downtime impact calculator.

Once the most pressing vulnerabilities are identified and prioritized, the network change management team can move forward with the configuring and testing of the patch that resolves the vulnerability.

CONFIGURING & TESTING NETWORK PATCHES

On August 23rd 2010, a Microsoft network infrastructure upgrade unexpectedly led to a two-hour period in which North American customers of the network suffered "intermittent" access.[7]

[5] *"PCI Compliance Guide". Fritz Young. http://www.pcicomplianceguide.org/*

[6] *"Impact of Network Downtime calculator" – Networks First and Warwick Business School. http://www.networksfirst.com/calculator/index.php*

[7] *"Meeting Your – And Our Own – Expectations" – Microsoft. September 2010 http://blogs.technet.com/b/msonline/archive/2010/09/08/meeting-your-and-our-own-expectations.aspx*

Microsoft had identified the vulnerability, prioritized it high enough to work on it, but did not sufficiently test and configure the patch.

Arguably, the most time-consuming function of a vulnerability management process is the configuring and testing of patches. Here, the NOC must weigh the time it takes to perform several tests against the severity of the vulnerability. It may be imperative to delay the more in-depth tests until after a patch is deployed. In any case, it's always advisable to perform a thorough test of the patch as soon as possible.

NOC testers typically use the following methods:

- Patch acceptance testing – verifying the specific patch fix against various configurations
  - >> Benefits
    - » Fastest testing method because it doesn't require a full network test environment and testing can be targeted to a specific vulnerability.
    - » Gives a conclusive result that verifies if the patch fixes the actual vulnerability.
  - >> Consequences of delaying (deploying the patch, then testing)
    - » An organization must place its faith in an equipment provider that the patch fixes the reported vulnerability.
    - » Other methods of testing could be impacted.
  - >> When to delay
    - » The patch is needed due to an exploited vulnerability in production that impacts business-critical applications.

- Penetration testing – verifying the patch doesn't re-introduce previous vulnerabilities or contain new ones
  - >> Benefits
    - » May uncover additional vulnerabilities which can be patched at the same time.
    - » Includes many of the techniques utilized by hackers and computer worms (DoS, brute force attacks, etc).
  - >> Consequences of delaying
    - » The patch may introduce more severe vulnerabilities into the network.
  - >> When to delay
    - » The patch is needed for a vulnerability that has a high likelihood of impacting business-critical applications, but hasn't done so yet.

- Deployment testing – verifying the patch deployment itself doesn't result in unexpected downtime
  - >> Benefits
    - » Readies the patch for deployment.
    - » If using an automated deployment system, this method of testing identifies the configurations and devices not included in the deployment scope.

> “Businesses may be overconfident – doing a good job of planning but still experiencing difficulty during unexpected disruptions.”

- >> Consequences of delaying
  - » Deployment of the patch may result in unexpected downtime.
  - » Manual deployment may be needed for the configurations and devices not covered by the automatic deployment system.
- >> When to delay
  - » If the number of vulnerable devices is low.
  - » Similar deployments (same device-type and overall configuration) handled by the automatic deployment system occurred without issue and the automatic deployment system hasn’t changed.

- Stress/load testing – verifies the overall functionality of the device and software under heavy-utilization scenarios.

Businesses may be overconfident – doing a good job of planning but still experiencing difficulty during unexpected disruptions. This highlights the need for businesses to conduct regular continuity/disaster recovery (BC/DR) plan testing to be certain it works in order to shore up vulnerabilities that show up only under stress. – CDW 2010 Business Continuity Straw Poll.[8]

> “Canary™ also provides the capability to research patches and how they reacted in other organizations prior to the testing and deployment of them on their own network.”

- >> Benefits
  - » Identifies potential failure points and vulnerabilities that only occur when there is a lot of traffic on the network.
  - » Verifies the network capacity, which allows engineers to schedule device refreshes accordingly.
- >> Consequences of delaying
  - » Patch deployment without load testing could cause failures immediately in a high-traffic network.
- >> When to delay
  - » If the traffic on the network is currently low and is expected to remain the same or decline.

Some vulnerability management services such as S3’s Canary™ have functionality built in to help track the testing of patches. Canary™ also provides the capability to research patches and how they reacted in other organizations prior to the testing and deployment of them on their own network.

When the patch passes testing, a standard deployment method needs to be followed to ensure minimal disruption to business.

[8] *“CDW 2010 Business Continuity Straw Poll” – CDW. September 2010 http://webobjects.cdw.com/webobjects/media/pdf/newsroom/CDW-Business-Continuity-Report-0910.pdf*

> “Scheduling and executing the deployment of network patches often ends up as a tug-of-war between the NOC and owners of the business applications.”

DEPLOYMENT OF NETWORK PATCHES

Scheduling and executing the deployment of network patches often ends up as a tug-of-war between the NOC and owners of the business applications. On one side, the patch must be deployed to resolve vulnerabilities that could lead to downtime. On the other side, the patch deployment itself could result in downtime.

Multiple deployment methodologies exist:

- Reactive deployment – deploy the patch when the network is down due to an exploited vulnerability
  - >> Benefits
    - » If the vulnerability is never exploited then the uptime for the network is maximized.
    - » The system is already down, and the allocation of resources for deployment exists due to the severity of the downtime.
  - >> Consequences
    - » The risk of exploit will remain on the network until it’s fulfilled or the network is refreshed.
    - » Over time, the availability of the network will be less than if the patch was released proactively.

- Deploy when tested – deploy the patch as soon as it has passed testing
  - >> Benefits
    - » Ensures network and data security by mitigating vulnerabilities as soon as possible.
  - >> Consequences
    - » While security is the focus of this methodology, availability is not. Multiple scheduled downtimes for deployments will occur.

- Strategic deployment – bundling tested patches together, targeting specific highly-critical vulnerabilities, and waiting until the infancy of the patch has expired. (10-30 days after a patch is released[9])
  - >> Benefits
    - » If planned correctly, multiple tested patches for highly-critical vulnerabilities will occur within the same scheduled downtime window, minimizing the need for individually scheduled downtimes.
    - » The patch is more mature and is unlikely to have same-vulnerability patches follow it from the equipment provider.
  - >> Consequences
    - » Requires more planning as bundling, scheduling and tracking of deployments is required.
    - » An exploit will remain on the network until a strategic deployment occurs.

[9] *“Solaris Patch Management: Recommended Strategy”. February 2005. http://www.sun.com/blueprints/0205/819-1002.pdf*

establishing a vulnerability management process

Some vulnerability management services such as S3's Canary™ enable the NOC to easily identify which patches to bundle and include in the next scheduled deployment. Once the deployment has occurred an assessment of the network needs to happen to ensure all applicable vulnerabilities have been patched.

VERIFYING PATCH DEPLOYMENT

Too often, the verification step of a process gets ignored or delayed as it's seen as a lower priority to the other steps. By ignoring this step, an organization cannot be sure that the patch was successfully deployed across the entire network. Even when using automated deployment systems, not every deployment will be successful.

Deployments can fail due to the following:

- Device is not available (it may be down or behind a firewall with no access to the deployment system).
- A different configuration was discovered that doesn't meet the conditions of the deployment system.
- If performed manually, the system administrator is not available.

The identification method used when first discovering the vulnerability should be performed again to verify the vulnerability no longer exists.

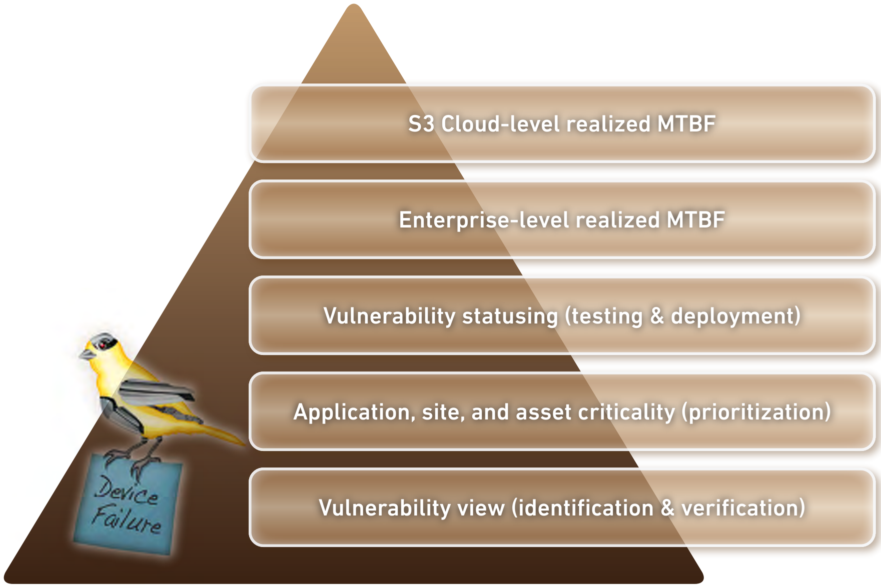
summary

There are many decisions to make when building a vulnerability management program from scratch. The number of devices in a network and criticality of the business applications running over the devices can dictate the methodologies used to identify, prioritize, test, and deploy vulnerability patches.

A small network without critical applications can get by with vulnerability assessments, limited testing, and reactive deployment. A larger or more critical network may want to look at automatic vulnerability identification & prioritization, stress testing, and strategic deployment.

No matter what methodologies are used, true vulnerabilities in a network should be addressed, patched, and verified to ensure maximum uptime. S3's Canary™ helps the tracking of vulnerabilities to ensure each one is taken care of in a reasonable time and risk is minimized.

about S3


S3 Cloud-level realized MTBF
Enterprise-level realized MTBF
Vulnerability statusing (testing & deployment)
Application, site, and asset criticality (prioritization)
Vulnerability view (identification & verification)
Device Failure

Canary™ consists of five product 'phases', beginning with vulnerability identification and verification, to ensure network uptime.

S3 provides back-office solutions to enterprises and network outsourcers to help manage network change, telecom expenses, and service requests.

Canary™ is S3's Early Warning System to assist in predicting network health while helping to prevent device failures and network outages. Canary™ has 5 phases to migrate a NOC from being reactive to being proactive.

At the first phase, Canary™ provides a vulnerability identification service. Based on vulnerabilties gathered from multiple sources and network scan data, Canary™ provides up-to-date insight into where vulnerabilties exist.

The second phase allows organizations to prioritize vulnerabilities based on the business-centric impact of the vulnerability.

The third phase allows statusing of vulnerabilities through the testing and deployment lifecycle.

Canary™'s fourth phase calculates a realized MTBF and provide a predicted date of demise for each device in the network. This helps the NOC understand which devices to replace next and which ones to build redundancy in for.

Canary™'s fifth phase is a subscription service between all of S3's clients to share the calculated realized MTBF between their networks. This allows technical designers to understand the true failure rates of devices before introducting them into their network.

For more information, please contact:

S3 Matching Technologies
7800 N. Mopac Expressway
Austin, TX 78759
512-329-3245