SECURITY INFORMATICS

Regional Centre of Excellence for Application Security, Lucknow

INSIDE THIS ISSUE

Security Informatics

A Quarterly Publication

January 2024- March 2024

Regional Centre of Excellence for Application Security, Lucknow

Under the immense leadership of

Shri V.T.V. Ramana
Dy. Director General
&
HOG, CoE-AppSec

&

Shri Sunil Sharma
Dy. Director General
&
SIO, NIC Uttar Pradesh

Under the able direction of
Shailesh Kumar Srivastava
HoD, CoEAS-UP & *Senior Director (IT)*

Team Members

Ravikar Srivastava, *Deputy Director (IT)*
Aparna Khare, *Deputy Director (IT)*
Rohit Sharma, *Deputy Director (IT)*
Divyanshi Kushwaha, *Deputy Director (IT)*
Aviral Awasthi, *Assistant Director (IT)*

Introduction

As the National Informatics Centre continues to advance its initiatives in the development and deployment of a diverse range of web and mobile applications leveraging cutting-edge technologies, there is a parallel mandate of security audits and penetration testing. This mandate is necessary for the security of applications and data associated. The huge number of applications in the purview of National Informatics Centre rises the need of third party security audits to fasten up the process. This demand is a response to the dynamic landscape of cyber threats that pose risks within the digital realm. Once the vulnerabilities found during third party audit activities are patched the vulnerability space is reduced making it easier for final audit. Tools such as AppScans are used to perform the audit procedure. Apart from this the infrastructure scan and penetration testing pipelined with this provides robust security compliance. These security activities are essential to counter evolving cyber threats and protect sensitive data. The Regional Centre of Excellence for Application Security, strategically located in Lucknow, plays a pivotal role in upholding these security standards, safeguarding the digital infrastructure across seven states in its jurisdiction and reinforcing the nation's resilience against potential threats.

The Regional Centre of Excellence for Application Security, Lucknow handles application security activities for seven states, namely, ***Uttar Pradesh, Uttarakhand, Himachal Pradesh, Punjab, Chandigarh and Jammu & Kashmir.***

Work Highlights

Centre Of Excellence for Application Security, Lucknow Work Highlights

ACTIVITIES UNDERTAKEN

Several activities were undertaken to enhance the safety and security of web applications, including infrastructure scans (200+), penetration testing, black box audits and white box audits, manual audits, SSL compliance scans, and development of modules for CoEAS applications (ASTS and ASAMS). More than 100 tickets were raised in this quarter highlighting various vulnerabilities in application. Apart from this around 30 Third party audit clearance has been given.

THIRD PARTY SECURITY AUDIT

As the number of applications are growing day by day, a third-party audit framework is a necessity. An entrusted third-party organization performs a through security audit which is then rechecked before providing clearance. AppScan tool is used to perform this activity. Using this tool, Major vulnerabilities such as cross site scripting, SQL injection, CSRF, etc. are checked. Only these major vulnerabilities are checked as thorough assessment of entire source code is already done during third party scan. HCL AppScan Standard functions as a Dynamic Analysis tool that assesses application security in real-time by simulating attacks on the application, mirroring methods akin to those employed by hackers. The test outcomes comprise a comprehensive dataset encompassing application inventory and intricate attack traffic, which can be replicated for validation and resolution. This data is accessible for scrutiny and manipulation within the user interface or exportable in multiple formats for utilization in other tools.

Recent Incidents

‘ArcaneDoor’ Cyberspies Hacked Cisco Firewalls

Image Source https://www.uctoday.com/collaboration/cisco-patches-two-high-risk-ios-software-threats/

Firewalls are meant to be digital fortresses, but hackers are turning them into gateways. Cisco recently revealed that state-sponsored spies exploited zero-day vulnerabilities in their own firewalls to breach government networks around the world. This attack, known as 'ArcaneDoor', highlights the increasing vulnerability of even the most trusted security systems.

Working with victims and intelligence partners, Cisco uncovered a sophisticated attack chain that was used to implant custom malware and execute commands across a small set of customers. During investigation, it was identified that a previously unknown actor now tracked as UAT4356 by Talos and STORM-1849 by the Microsoft Threat Intelligence Center was behind this attack. This actor utilized an in-depth knowledge of the devices that they targeted. UAT4356 deployed two backdoors, “Line Runner” and “Line Dancer,” which were used collectively to conduct malicious actions on-target, which included configuration modification, reconnaissance, network traffic capture/exfiltration and potentially lateral movement.

Resources for Further Reading:

https://www.cisa.gov/news-events/alerts/2024/04/24/cisco-releases-security-updates-addressing-arcanedoor-vulnerabilities-cisco-firewall-platforms

Knowledge Hub

Zero Trust Strategy

According to a latest report published by Gartner, over 50% of the organizations across the world has implemented Zero Trust strategy whether partly or fully. More that half of this group stated that zero trust approach is considered as "industry best practice". But majority organizations are not sure what top practices are for zero-trust implementation as per a recent survey.

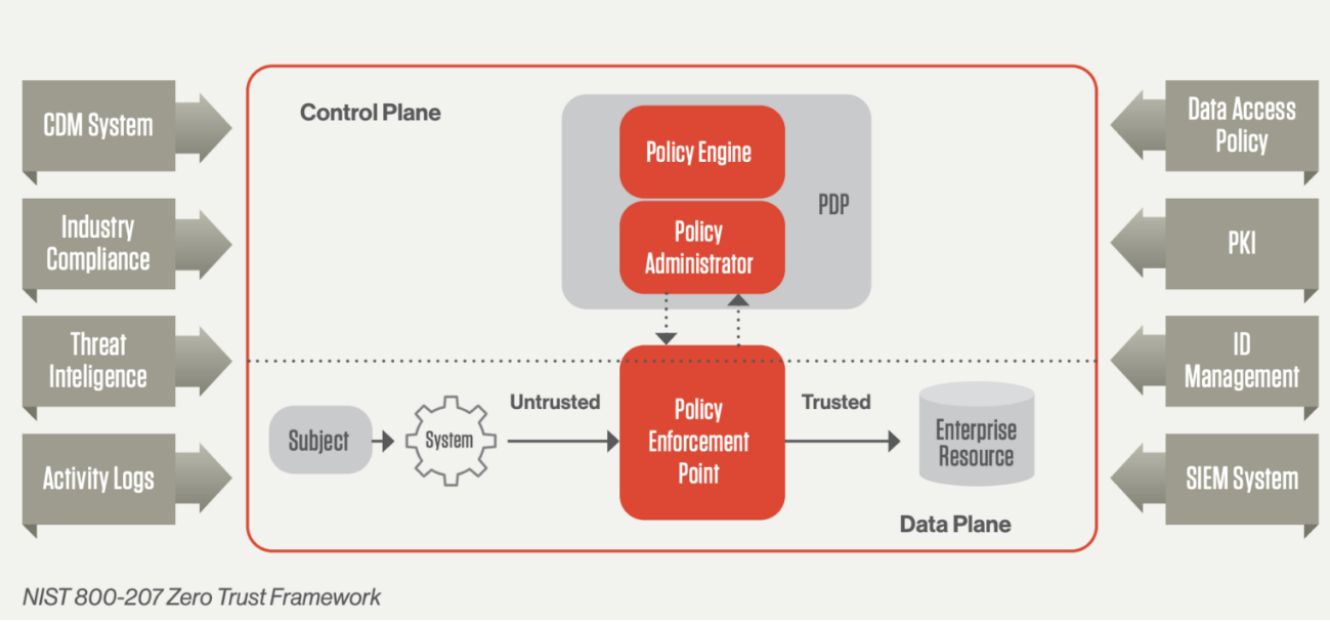
Experts has few recommendations to implement zero trust strategy -recognize the scope of what it can reasonably cover (which usually is not the entirety of an organization), incorporate metrics to measure success and risk.

WHAT IS ZERO TRUST?

Zero trust is a security framework in which every end point or user (whether inside or outside the organization) needs to be authenticated, authorized and continuously validated for security configuration and posture before granting any access to application and data. It is a framework for securing infrastructure and data in today's modern digital transformation.

Zero trust seeks to address the following principles:

1) Continuous Verification- Always verify access, all the time, for all the resources.
2) Limit the "Blast Radius"- Minimize impact if an external or insider breach occur.
3) Automate context collection and response- Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate response.



NIST 800-207 Zero Trust Framework

Image Source https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

HOW ZERO TRUST WORKS?

Zero Trust framework works by combining technologies such as risk based multi factor authentication, identity protection, next generation endpoint security, and robust cloud workload technology to verify a user or systems identity, consideration of access at that moment in time, and the maintenance of system security. Zero Trust also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications.

KEY PRINCIPLES OF ZERO TRUST

1) **Never Trust, Always Verify:** Zero Trust mandates continuous authentication and authorization of every user, device, and connection attempting to access resources. This eliminates assumptions about trustworthiness based solely on location within the network.
2) **Least Privilege Access:** The principle of least privilege states that users and devices should only have the minimum level of access necessary to perform their functions. This limits the potential damage if an account or device is compromised.
3) **Microsegmentation:** Zero Trust advocates breaking the network down into smaller, isolated segments. This granular approach restricts lateral movement, making it more difficult for attackers to spread throughout the network.

COMPONENTS OF A ZERO TRUST ARCHITECTURE

- Identity and Access Management (IAM): A robust IAM system is crucial for enforcing Zero Trust. It ensures that only authorized users and devices can access resources, and that their access is aligned with the principle of least privilege.
- Device Security: Each device connecting to the network must be verified. This includes laptops, desktops, mobile devices, and IoT devices. Security measures encompass posture checks, multi-factor authentication, and device health assessments.
- Workload Security: Workloads, whether running on physical servers, virtual machines, or in the cloud, must be secured. This involves vulnerability management, patching, and application whitelisting.
- Workload Security: Workloads, whether running on physical servers, virtual machines, or in the cloud, must be secured. This involves vulnerability management, patching, and application whitelisting.
- Workload Security: Workloads, whether running on physical servers, virtual machines, or in the cloud, must be secured. This involves vulnerability management, patching, and application whitelisting.
- Workload Security: Workloads, whether running on physical servers, virtual machines, or in the cloud, must be secured. This involves vulnerability management, patching, and application whitelisting.

IMPLEMENTING ZERO TRUST

- Discovery and Assessment: Identify all sensitive assets, data flows, and users requiring access. Assess your current security posture.
- Policy Development: Create strong and granular access policies based on the principles of Zero Trust.
- Technology Implementation: Select and deploy appropriate Zero Trust technologies, such as software-defined perimeters (SDPs), next-generation firewalls (NGFWs), and IAM solutions.
- Monitoring and Optimization: Continuously monitor network activity, refine policies, and adapt your Zero Trust implementation to meet evolving security requirements.

BENEFITS OF ZERO TRUST

- Improved Security Posture: Zero Trust significantly improves an organization's overall security stance against both internal and external threats.
- Reduced Attack Surface: Limiting access and isolating resources reduces the attack surface attackers can exploit.
- Enhanced Compliance: Zero Trust principles align with numerous regulatory frameworks, making compliance easier to demonstrate.

Advisories

List of Advisories

- **Regularly Update and Patch**: Always keep your server operating systems, software, databases, and all web platforms (like WordPress, Joomla) up to date. Many attacks exploit known vulnerabilities in outdated software.
- **Use HTTPS:** Implement SSL/TLS to encrypt data between the client and server. This prevents man-in-the-middle attacks and ensures data integrity.
- **Input Validation**: Always validate and sanitize inputs to prevent SQL injection, script injection, and other injection attacks. Inputs include form data, URLs, and any data from external sources.
- **Implement Content Security Policy (CSP):** This helps prevent cross-site scripting (XSS) by controlling which resources can be loaded.
- **Secure Password Policies**: Enforce strong password policies for users. Implement multi-factor authentication wherever possible.
- **Session Management**: Use secure methods for session management. Ensure session IDs are randomly generated, use HTTPS for transmitting session cookies, and set the "HttpOnly" and "Secure" flags for cookies.
- **Limit Rate of Requests**: Implement rate limiting to prevent brute force attacks on login and other transactional operations.
- **Least Privilege Principle**: Ensure that software components run with the least privilege necessary. If a component only needs read access to a database, do not give it write access.

Any Suggestions/Feedback feel free to write:

Shailesh Kumar Srivastava
HoD, CoEAS-Lucknow
Email - **shailesh.srivastava@nic.in**
IP Phone- **47055**