Trust No One

Zero Trust – Iz X Files u stvarnost

NetPP TECHNOLOGY

Srđan Vranić

Perimeter Security (Outbound traffic)

- List of Allowed Applications in a company
- User identification
- Decryption
- IPS
- Prevention of C2 communication
- DNS Security
- Geolocation
- DLP / Data filtering
- File blocking
- URL filtering
- Block user credential submissions
- Sandboxing
- Control traffic from IoT devices
- Control User/Device behaviour, automated isolation
- XDR

Perimeter Security (Inbound traffic)

- List of Allowed Applications in a company
- Inbound decryption
- IPS
- Geolocation
- DDOS prevention
- Flooding prevention
- Continuous monitoring of externally visible vulnerabilities
- Continuous monitoring of all vulnerabilities and their prioritization
- Phishing prevention/Mail security
- Sandboxing
- Micro-segmentation
- Application security
- MFA
- XDR

Data Center Security

- List of Allowed Applications in a company
- User identification
- Decryption
- Flooding prevention
- Continuous monitoring of all vulnerabilities and their prioritization
- Sandboxing
- User/Device behaviour, automated isolation
- IPS
- Control IoT vulnerabilities
- Micro-segmentation
- Application security
- MFA
- XDR
- Regular patching
- Awareness of service/app/data criticality
- Physical security and access procedures
- Privileged Access Management
- Encryption for data in use/rest/transit

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

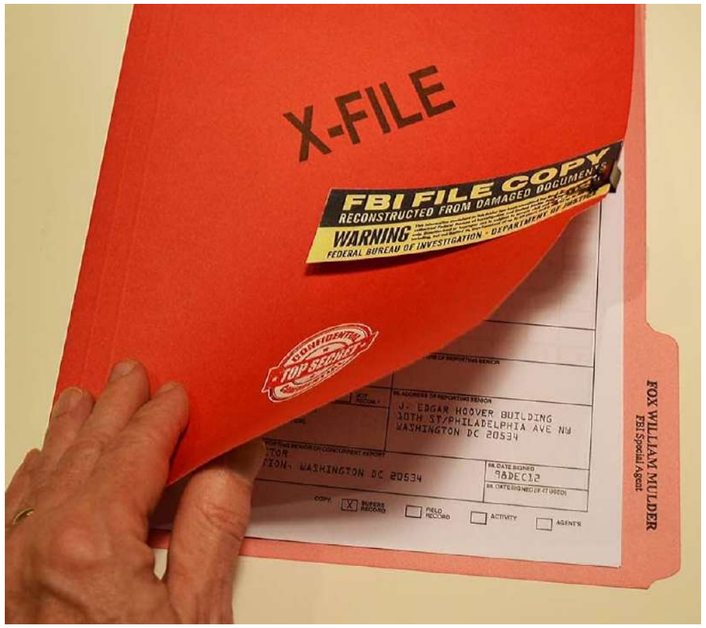
liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has

EO 14028



NetOne TECHNOLOGY

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-207

Zero Trust Architecture

NetOO TECHNOLOGY

What does Zero Trust bring us?

- No implicit trust
- Where is the Perimeter?
- Focus is on protecting resources not network segments
- Inside-Out architecture
- Crown Jewels
- Access to resources with minimal privileges
- Access to resources – session based
- Authentication and authorization (crucial)
- Device security posture
- Secure communication
- Limit internal lateral movement during security breach
- Do not consider enterprise network as a trust zone
- Continuous diagnostic and mitigation
- ZT vs ZTA

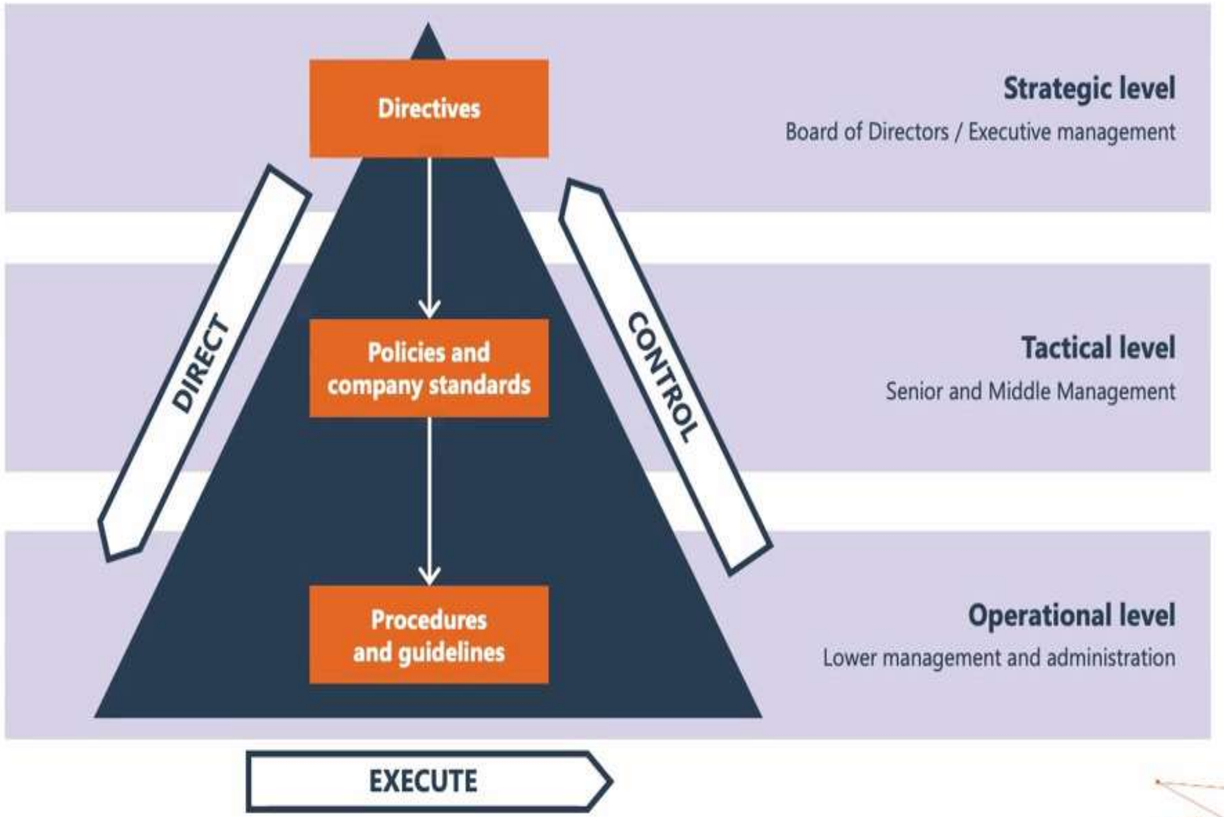
Zero Trust

- Complete visibility
- Complete inspection
- Complete logging

- Zero Trust for Users
- Zero Trust for Applications
- Zero Trust for Infrastructure

- Identity (Authentication, authorization, MFA, PAM, Anomaly detection)
- Devices (Inventory, Device tracking, Manage risk from unauthorized devices, Prevent access from non-compliant devices)
- Networks (Micro-segmentation, Micro-perimeters, IPS, Adopt strong encryption)
- Applications (SAST, DAST)
- Data (Focus on high/value and sensitive data, Encryption for data in use/rest/transit, DLP)

Zero Trust
(How to start)



Zero Trust (Readiness Assessment)

Assessment (Strategic, Managerial, Operational)

The Readiness assessment is executed by means of a workshop in which questionnaires are entered in the Zero trust tool that calculates the maturity scores and averages. Workshops can also be done online. The following audience should be involved in the assessment; C-Level (Executive management): IT Director, CIO, CTO, CISO. Involvement to determine Cybersecurity strategy, critical assets and value chains, DAAS processes, reporting mechanisms, applicable organizational policies and standards for compliance.

Strategic: Understanding the organizational environment (context) and capabilities. Defining the current and the desired state.

Managerial: Understanding managerial security and risk processes and structures (committees and reporting lines). Defining the current and the desired state.

Operational: Understanding the basic operational processes that utilize Zero trust in your technical environment. Defining the current and the desired state.

Level	Criteria
5 Optimized	High Quality, proven full link with business objectives, measured with metrics, continuous improvement and provides platform for agility and innovation
4 Predictable	Effectiveness is proven via control cycles, and are based on standards, processes are measured and reported. Budgets are defined and managed.
3 Established	Implementation is proven, organization wide standards in place in design.
2 Managed	Managed via ad-hoc projects,
1 Performed	Something informal in place and achieves its purpose. Work is delayed and often over budget

Zero Trust (Maturity Model)

SOC

- Integration of different security tools from different vendors
- Full automation
- Threat hunting
- 24x7 coverage

HVALA NA PAŽNJI

+381 11 36999 967
www.netpp.rs
Otokara Keršovanija 11/39, Beograd