Win the Cyberwar With Zero Trust

John Kindervag

Field CTO
The Four Levels of War

Grand Strategy (Political)

The Ultimate Goal
Grand Strategy - WWII
Strategy - WWII
Strategy - WWII
The Four Levels of War

Grand Strategy (Political)

Strategy

Tactics

The Ultimate Goal

The Big Idea

The Things You Use
Tactics - WWII
The Four Levels of War

Grand Strategy (Political)

The Ultimate Goal

Strategy

The Big Idea

Tactics

The Things You Use

Operations

The Way You Use Them
Operations - WWII
The Four Levels of Cyberwar

**Grand Strategy (Political)**
- Stop Data Breaches

**Strategy**
- Zero Trust

**Tactics**
- Tools/Policies

**Operations**
- Platform
Cyber Security Grand Strategy: Prevent Data Breaches

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE  DEC. 13, 2015

Verizon, Yahoo Near Revised Deal That Cuts Price of Web Firm by About $300 Million

Companies are discussing splitting any future liabilities as a result of Yahoo data-breach hacks.

By JENA KASHKOU and ROY DEVEREUX
Updated Dec. 16, 2013 4:30 p.m. ET

Target Hit by Credit-Card Breach

Customers' Info May Have Been Stolen Over Black Friday Weekend

By ROBIN S. JOSEPH, DEEPIK VADNIA and RENA GERMANO
Updated Dec. 16, 2013 7:49 p.m. ET
Federal Insider

Hacks of OPM databases compromised 22.1 million people, federal authorities say

By Ellen Nakashima  July 9, 2015  

WASHINGTON — Federal agencies seeking to stop another major hack of Americans’ personal data must establish a “zero trust” system that treats government employees as just as big a threat to cybersecurity as foreign attackers, says a report being released Wednesday by a House panel.

“The zero trust model centers on the concept that users inside a network are no more trustworthy than users outside a network,” says the 231-page report by the Oversight and Government Reform Committee’s Republican majority.

The document is the culmination of a year-long investigation by the panel into the massive cyber attacks against the U.S. Office of Personnel Management that compromised the personal data of more than 22 million Americans.

The report recommends that federal agencies enforce stricter controls over access to their computer networks by employees and government contractors. The OPM breaches raised questions about the security of government contractors. Two
Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM’s network, and ultimately accessed the “crown jewel” data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a “zero trust” model of information security and IT

83 Gov’t Accountability Office, GAO-11-634, Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management (Oct. 2011) (stating the average CIO’s tenure is two years).
The Four Levels of Cyberwar

Grand Strategy (Political)

Strategy

Tactics

Operations

Stop Data Breaches

Zero Trust

Tools/Policies

Platform
Not a Strategy

Not a Strategy
Not a Strategy
Not a Strategy

John Kindervag
@Kindervag

Most companies use HOPE as their risk mitigation strategy:
(H)ead in the sand
(O)bfuscate reality
(P)oint the finger
(E)mployment journey
TRUST is a dangerous VULNERABILITY that is EXPLOITED by MALICIOUS actors
Which one goes to the internet?

Zero Trust

Zero Trust Design Concepts

• Focus on the business outcomes
• Design from the Inside > Out
  • Start with the assets or data that need protection
• Determine who or what needs access
  • Need to know/Least-privilege
• Inspect and log all traffic
1. Who the President is...
2. Where the President is...
3. Who should have access to the President...
Zero Trust
Zero Trust is the answer!

NEW YORK — Google Inc [GOOGL-0.31%] CIO Ben Fried says the company is moving away from the idea of a corporate network to an infrastructure that reflects the habits and security of Internet users. “You have the idea of a private network that lives inside the data center and a few servers, but really you want to treat all of the ways that people connect to you as if it were the Internet,” Mr. Fried said at a panel at the Bloomberg Enterprise Technology Summit.

The wave of the future is building or adopting enterprise infrastructure that is essentially “zero trust.” Enterprises will need to build infrastructures with the assumptions that people are connecting to a network that can be trusted no...
The Four Levels of Cyberwar

- **Grand Strategy (Political)**
- **Strategy**
- **Tactics**
- **Operations**

- **Stop Data Breaches**
- **Zero Trust**
- **Tools/Policies**
- **Platform**
DELIVERING THE NEXT-GENERATION SECURITY PLATFORM
EXPANSIVE PARTNER ECOSYSTEM

Over 120 Technology Integrations

Open APIs

Extensive Ecosystem of Partners Across Multiple Technologies

Virtualization
Cloud
Networking
Mobility
Security
Analytics
Enterprise Security
Identity and Access Management
SD-WAN Orchestration & Security
Threat Intelligence
Over 120 Technology Integrations
Open APIs
Extensive Ecosystem of Partners Across Multiple Technologies
Augment Hierarchal Networks with Zero Trust

Extend Zero Trust to the Public Cloud

Public Cloud

Workload
Hypervisor
VM NGFW
Virtual Net
vSwitch
PSY Switch

Virtualization MGMT
PSY MGMT

VM Series NGFW
Virtual Network
vSwitch
PA Series NGFW
Panorama
The Four Levels of Cyberwar

- Grand Strategy (Political)
  - Stop Data Breaches
- Strategy
  - Zero Trust
- Tactics
  - Tools/Policies
- Operations
  - Platform
Automation and Orchestration
AUTOMATED SECURITY ACTIONS

1. Granular log filtering
2. Automated actions on the NGFW
3. Automated actions on third party systems

Threat Prevention logs
Malware and phishing logs
Correlated Event logs
System logs
Data filtering logs
Traps logs
...

10.3.4.122
Compromised
Dynamic Address Group
Enforce multi-factor authentication

Policy | Source | Action
--- | --- | ---
Compromised hosts | Dynamic Address Group | Enforce multi-factor authentication

Any REST API

© 2017 Palo Alto Networks, Inc. Confidential
The Four Levels of Cyberwar

**Grand Strategy (Political)**
- Stop Data Breaches

**Strategy**
- Zero Trust

**Tactics**
- Tools/Policies

**Operations**
- Platform
Rep. Jason Chaffetz on Zero Trust:

“Zero trust would have profoundly limited the attacker’s ability to move within OPM’s network and access such sensitive data.”

Thank You

John Kindervag
Field CTO
jkindervag@paloaltonetworks.com
@Kindervag