CONTAINING NATIONAL CYBER RISK DEPENDS ON CONSOLIDATED SECURITY ARCHITECTURE

Sponsored by Cyber Talk

Containing National Cyber Risk Depends on Consolidated Security Architecture

Introduction

In the face of ongoing cyber attacks against national governments, it's clear that ineffective cyber security measures can impact a country's military defenses, economic health, critical infrastructure, and foreign policy. And this trend is showing little sign of abating.

One of the most egregious cyber attacks acknowledged by the US Government is the recent SolarWinds attack that breached nine federal agencies. Attackers stole information related to intelligence investigations, sanctions on Russian citizens, responses to COVID-19, and more. This attack exploited weaknesses in SolarWinds and Microsoft Office 365 software.[1] It's speculated that 'Havana Syndrome' attacks on key US and Canadian diplomats are being fueled by "advance knowledge of US official trips and the locations of US diplomats and intelligence agents."[2] Additionally, it's possible that this sensitive information could be leaking from government emails and calendars served from government data centers and Office 365 in the cloud. Adversaries could be using compromised smartphones as tracking devices to spy on meetings through smartphones' microphones and cameras.

The U.S. government isn't alone.

Threat actors compromised the French government's visa system exposing the nationalities, birth dates, passport numbers and other personal information of people who applied for French visas.[3] Cyber attacks in France have increased fourfold within a year.[4] Likewise, Japanese government agencies suffered data breaches when threat actors compromised Fujitsu's "ProjectWEB" cloud-based (SaaS) information sharing tool.[5] Attacks on governments around the world are increasing.

---

[1] Joseph Menn and Christopher Bing, Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes, Reuters, October 8, 2021. https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/

[2] Seth J. Frantzman, 'Havana syndrome' attacks reveal US adversaries may have dangerous intel, Jerusalem Post, October 17, 2021. https://www.jpost.com/international/havana-syndrome-attacks-reveal-us-adversaries-may-have-dangerous-intel-682235

[3] Adam Bannister, French government visa website hit by cyber-attack that exposed applicants' personal data, The Daily Swig, September 7, 2021. https://portswigger.net/daily-swig/french-government-visa-website-hit-by-cyber-attack-that-exposed-applicants-personal-data

[4] Anon, Cyber-attacks quadrupled in France in the space of a year, RFI, May 3, 2021. https://www.rfi.fr/en/france/20210305-cyber-attacks-quadrupled-in-france-in-the-space-of-a-year-security-military-defence

[5] Alicia Hope, Japanese Government Agencies Suffered Cyber Attack Exposing Proprietary Data, CPO Magazine, June 3, 2021. https://www.cpomagazine.com/cyber-security/japanese-government-agencies-suffered-cyber-attack-exposing-proprietary-data

Current Defenses

Although different countries use different strategies, the U.S. Cyber Security & Infrastructure Security Agency (CISA) provides the Einstein system as "baseline security" for Federal Civilian Executive Branch (FCEB) and other agencies.[6] Einstein is an intrusion detection/prevention system (ID/IP) that analyzes traffic as it enters the network and compares the traffic against a list of known threat signatures. If Einstein detects a threat, it generates an alert so the threat can be removed and damage can be mitigated. The problems with this system are twofold: new, unknown attacks that lack signatures evade detection as do polymorphic malware that change their code as they travel through a network environment. Also, Einstein lets known threats pass into a system where the threats can move through the system, inflicting damage until detected and stopped. Einstein provides outdated 3rd-generation protection against today's advanced 5th generation multivector, polymorphic threats.

The problem shared by government agencies and departments around the world, is that they process workloads in their data centers, in the cloud, SaaS, on smart phones and other mobile devices as well as IoT devices. Experts have estimated that it can take 60 or more different kinds of security controls to fully protect today's government entities. Trying to provide full-environment security using point solutions that are not compatible and interoperable is complex, making it virtually undoable.

However, there is an answer.

Consolidated Security Architecture

Using a large patchwork of point solutions for cyber security is overly complex end-to-end from: purchasing, deployment, management and administration, reporting and tech support. The alternative is to deploy the security controls you need within a consolidated security architecture framework. It's advantages are as follows:

1. Purchasing and tech support come from a single source.
2. Straightforward deployment with all systems purpose-built to be compatible and interoperable, sharing threat information across data centers, cloud, endpoints, phones and the rest.
3. Streamlined security management and administration is through a single user interface for all security controls, reducing the number of staff-hours needed while improving event response and compliance reporting.

Additionally, a consolidated or unified security architecture can ease the implementation of advanced threat prevention assisted by using artificial intelligence throughout the entire computing environment for much more effective security.

---

[6] Anon, Einstein, CISA. Gov. https://www.cisa.gov/einstein

Conclusion:

When you write your next Request for Information (RFI) or Request for Quote (RFQ), be sure that you specify for

1. Consolidated security architecture that protects your datacenter, cloud, smartphones and mobile devices, endpoints, data security, SaaS and all other assets with a single unified user interface

2. Advanced threat prevention assisted by AI that stops malware outside your environment

Protect your own department or agency and influence your contractors to adopt this approach for effective protection, cost savings and simplified compliance.

Explore the possibilities with Check Point Infinity, a leading consolidated security architecture.

Additional Resources

Ax Sharma, US gov't will slap contractors with civil lawsuits for hiding breaches, Ars Technica, October 7, 2021.
https://arstechnica.com/information-technology/2021/10/us-govt-will-slap-contractors-with-civil-lawsuits-for-hiding-breaches

Frank Bajak, Microsoft: Russia behind 58% of detected state-backed hacks, AP News, October 7, 2021.
https://apnews.com/article/technology-business-china-europe-united-states-e13548edf082992a735a0af1da39b6c8

Zev Stub, Newly-found Iranian cyber-espionage may pose 'real threat' to Israel, Jerusalem Post, October 7, 2021.
https://www.jpost.com/jpost-tech/newly-found-iranian-cyber-espionage-may-pose-real-threat-to-israel-681196

Zack Whittaker, A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen Lab, Tech Crunch, August 24, 2021.
https://techcrunch.com/2021/08/24/nso-pegasus-bahrain-iphone-security

Dan Sabbagh, NSO Pegasus spyware can no longer target UK phone numbers, The Guardian, October 8, 2021.
https://www.theguardian.com/world/2021/oct/08/nso-pegasus-spyware-can-no-longer-target-uk-phone-numbers

Sean Lyngaas, Microsoft says Iran-linked hackers have targeted US and Israeli defense firms, CNN, October 11, 2021.
https://www.cnn.com/2021/10/11/politics/microsoft-iran-hackers-defense-firms/index.html

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com