



White Paper

The 5 Things You Did NOT Know About Cybersecurity ...and MUST Know!

29 April 2021

Purpose

Industries, agencies, and companies have defined their own criteria and standards around cybersecurity practices. Leading ideas and concepts put forth by experts in their field have served as the foundation for many of these practices and standards. Over time, terms and meanings have been blurred with some manufacturer bias causing misconceptions in understanding, identifying, and implementing accurate, reliable cybersecurity. This paper serves the novice and experienced professional who set organizational standards, review cybersecurity posture, implement and manage cybersecurity. These are the 5 things you didn't know about cybersecurity ...and MUST know!

1. Validate Zero-Day Detection Claims... The Industry Is Not Straightforward

A Zero-Day exploit is a computer-software vulnerability mostly **unknown to those who should be interested in its mitigation** including the target software vendor. Until the vulnerability is corrected or mitigated (usually requires patching by software vendor), bad actors or hackers can take advantage of it to infiltrate systems and/or exfiltrate data with malicious intent.

There are two types of Zero-Day exploits:

1. **Not Discovered** by those who should be interested in its mitigation
2. **Discovered** but no vendor updates released or implemented to correct or mitigate the exploit

Keep in mind a Zero-Day exploit is closed only when a vendor has identified, developed, tested, released an update and that update is applied to all affected systems.

The danger of a Zero-Day (Not Discovered) is that bad actors develop, identify and/or exploit them before any cyber-solution relying on CVEs (Common Vulnerabilities and Exposures) or signatures can ever detect them. History has taught us that some Zero-Day exploits can go undetected by “those who should be interested in its mitigation” for a year or longer. This creates an unacceptable amount of dwell time and first strike capability for bad actors to infiltrate systems and exfiltrate data.

What you MUST know...

There are vendors in the cybersecurity space that currently claim Zero-Day detection. It is extremely rare to find a vendor solution that can detect and mitigate Type 1 Zero-Day (Not Discovered) exploits denoted above. The companies that do make this generic Zero-Day claim will typically identify and mitigate Type 2 Zero-Day (Discovered) exploits where the tactics, techniques, procedures have been exposed and a plan to mitigate, CVE, or signature has been created so a scanner can detect them. As noted above, someone needs to experience, research, and isolate the source of the Zero-Day, then report it to the vendor or community. Once the vendor receives news, they have to identify where the exploit exists, start a development cycle, test and QA the updates, wait for a release cycle (or single update if critical vulnerability), then release the update. Once the update is released, it must be applied to all systems. This cycle can take more than a year or longer where bad actors have the advantage to continue exploiting the vulnerability.

2. Virus Scanners Report "All Good / Clean"... Usually Not True

At one time or another a network or system administrator ran some type of network, infrastructure, or endpoint scan to detect viruses, ransomware, malware, and other vulnerabilities. The hopeful anticipation is to see a clean bill of health and green check marks denoting a cyber-healthy, clean environment. If there were some findings, they could usually be cleaned up in a couple days or weeks. Getting a clean, healthy report was the goal... but should it have been?

Today's ransomware and malware attacks have evolved to a point that industry solutions have a much more difficult time detecting encryption and file state changes in a reasonable timeframe to prevent an actual compromise.

- Attacks are happening faster than solution providers can identify the ransomware and incorporate into their scanning technologies (typically weeks or months before they are incorporated into a signature-based detection system or AI based filtering system).
- AI and / or API call monitoring technologies monitor known attacks and detect compromises after infiltration. AI takes too long to train against all the new daily variants and discovery is required to initiate training in any event.
- Industry scanners are not finding any embedded libraries-based attacks, and therefore the embedded attacks bypass almost all scanning technologies found in the market today.

The consequence is that new and evolving ransomware and malware attacks are now getting past even the biggest solution providers and leading scanners in the industry.

What you MUST know...

Staggering Facts:

- Hackers are developing 560,000 new malware variants daily. March 2021, DataProt.net
- Over 350,000 new malicious programs (malware) are registered daily. av-test.org
- Every minute four companies fall victim to ransomware attacks. March 2021, DataProt.net
- Leading antivirus scanners have a success rate between 51.1% to 98.7% (not considering "Zero-Day" exploits). av-comparatives.org report (malware protection test March 2019)
- ALL antivirus software showed some degree of scanner compromise by malware up to almost 10%. av-comparative.org report (enterprise, real-world protection scan Aug-Nov 2020)
- 75% of companies infected with ransomware were running up-to-date endpoint protection. Purplesec.us article

It is difficult to truly determine the actual effectiveness of antivirus scanners with the record numbers of infections reported, malware variants, Zero-Day malware exploits, and an excess of marketing. With the reduced rate of signatures to new variants, ineffectiveness and possible compromise of antivirus scanners, traditional methods must be questioned and scrutinized heavily. Be wary of scanning solutions that do not integrate with a network protection platform and provide security boundaries to isolate and eliminate the chance of scanner compromise by malware.

An Example: If a medium sized company is considered, they can easily have 10 Million files. A 98% success rate when scanning files leaves about 200,000 files compromised, at risk, or unscannable. This success rate is unacceptable protection in security-conscious environments.

What scanner technologies should an organization consider?

- Detects anomalies in the data by identifying ransomware, malware, and unknown encryption.
- Provides automated forensics process, that can detect both known and unknown forms of encryption and other tampering such as embedded files.
- Does NOT rely on monitoring APIs that call for encryption libraries to encrypt a file.
- Detects the file state of the encrypted file itself.
- Integrates with a network protection platform to isolate/eliminate possibility of a compromise
- Can scale from small amounts of data to exabytes in a large enterprise.
- Continuously scans and crawls through the data to revalidate.

3. Zero Trust Should Be Easy, Why Can't We Just "Turn It On or Enable It."

Many perceive Zero Trust as a way of restricting access to networks and systems by checking a box or switching it on in software or cloud services. The truth is that proper implementation of Zero Trust in an environment goes much deeper and touches every layer and level. Below are some standard definitions and guidance to navigate the multitude of vendor offerings around Zero Trust.

Defined by the NSA's Guidance on Zero Trust Security Model: "The Zero Trust model eliminates trust in any one element, node, or service by assuming that a breach is inevitable or has already occurred. The data-centric security model constantly limits access while also looking for anomalous or malicious activity."

What you MUST know...

Zero Trust should be implemented using a design where all of the solutions assume they exist in a hostile environment. The solutions operate as if other layers in a company's protections have been compromised. This allows isolation of the different layers to improve protection by combining the Zero Trust principles throughout the environment from perimeters to VPNs, remote access to Web Servers and applications.

For a true Zero Trust enabled environment, focus on companies and solutions that evaluate as "Advanced" in NSA's Zero Trust Maturity Model; as defined in NSA's Cybersecurity Paper - Embracing a Zero Trust Security Model. This means that Solution Providers should be able to deploy advanced protections and controls with robust analytics and orchestration.

Be wary of consolidated software solutions containing security or security controls that do "everything" in one place. These types of solutions, albeit low cost and easy to deploy, do not provide the proper boundaries if another layer or component was compromised or breached. Example: If a hypervisor hosting network, firewall, webserver, etc. is compromised (Hyperjacking), then ALL services, virtual machines, and/or layers are also compromised. Hypervisors do have their place in datacenters, but proper security boundaries must be considered for a successful Zero Trust model.

4. Our Remote Workforce Uses VPNs And Are VERY Secure... Or Are They?

Most organizations rely on traditional VPNs, digital certificates / secure keys, and CAs (Certificate Authorities) to issue or hold those certs for securing their private networks and remote workforce. The cyber-landscape is evolving with faster processing, more aggressive / frequent attacks, and more attack surfaces which better enable breaches leaving everyone vulnerable. Traditional VPNs are NOT as secure as everyone would hope.

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols, encryption techniques, and digital certificates or secure keys.

What you MUST know...

VPN hacks became successful back in 2019 and soon after CAs were being compromised as well. This has been reported to and recognized by high-level agencies and the industry seems to keep this quiet since almost all companies are using traditional VPNs for remote users and CAs are not secure and may be at risk or already compromised.

When a CA is hacked, the bad actors can get private digital certificates and literally walk right in the front door of a company and gain access to any or all systems!

IPSec has been adopted for its ease of securing network-to-network tunnels (datacenters), but SSLs are accepted as a more secure method for remote user VPNs since it works at layers above those of IPSec.

Network-to-network tunnels often use passwords or digital certificates. They permanently store the keys to allow the tunnel to establish automatically, without intervention from the administrator.

How can an organization protect their remote users?

A different approach is needed to solve the many cybersecurity threats faced today. This will require full integration and / or replacement of some existing cybersecurity systems to ones that understand the complete end-to-end threats across our network.

Consider VPN technologies that use the highest levels of encryption and non-permanent keys to maintain confidentiality and security. By using keys that are not permanently stored (generated and held by compromised CA's), attackers cannot gain access to the VPNs.

Multi-Factor Authentication (MFA) along with passwords, biometrics, or other cryptographic methods should always be sought out when deciding on a VPN technology.

Invest in a solution that can grow with the organization, and as the attacks gain sophistication to defend against them with a machine-driven, automated defense technology.

5. Most Companies Take 8 Months Or More To Contain A Breach

An implemented and rehearsed Incident Response Plan (IRP) seems the best way of mitigating and minimizing time back to normal operations. The challenge with this approach is waiting for a compromise before mitigation. Protection is needed that preemptively defends against Zero-Day attacks, Sleeper Malware, and other stealthy types of attacks. Until the technology ensures a breach is completely contained in seconds, other systems can be infiltrated and sensitive data can be exfiltrated. The reasons lie in most of the items outlined above in this white paper:

- **Zero-Day exploits** can live in software for over a year and expose systems to a myriad of attacks
- **Ransomware and Malware infections** are exponentially rising with 560,000 new malware variants detected daily. Every minute, four companies fall victim to ransomware attacks.
- **Tactics, Techniques, Procedures (TTPs)** used are much faster and much more sophisticated.
- **Countless potential attack surfaces** are created from tens of thousands of laptops, desktops, servers, cameras, sensors, phones, and more exposed to networks and internet.

“280 days: Average time to identify and contain a breach” – IBM (How much would a data breach cost your business?)

“An uncomfortable truth has been recently revealed: on average, a company data breach stays undiscovered for a shocking 197 days—more than 6 months. Frustratingly, it takes another 69 days (over 2 months) to fix the problem.” – MacKeeper (Data Lost in Breach? You’ll Likely Learn About It in 6 Months or More.)

What you MUST know...

The two critical principles for preventing and containing breaches stem from the “C-I-A Triad”: Confidentiality and Integrity. Below are a few key points and some recommendations.

Confidentiality: Most cyber solutions use point products or attempt to encapsulate many layers into a single platform to save cost. The most effective solution is one that employs proper security boundaries in a Defense-in-Depth blueprint model to enable a Zero Trust environment.

Integrity: A number of vendors advocate the use of Snapshots or Versioning on storage to maintain Integrity. If used in a real-world scenario, eradicating two years of data to get back to a known, good state would be devastating to any organization! Example: A breach is initiated by a Social Engineering Attack where a user clicks on a link and a file is downloaded which includes sleeper malware to a network share. These can sit for one, two or more years and when woken up can leave other files and data locked or corrupt while still infiltrating systems and / or exfiltrating data.

How can an organization implement Confidentiality and Integrity for breach prevention?

- **Automated, pre-emptive cybersecurity solutions** possess the greatest potential in thwarting attacks and rapidly identifying any security breaches to reduce time and cost.
- **Use a Defense-in-Depth blueprint** for cybersecurity to: enable a Zero Trust environment, establish proper security boundaries, provide Confidentiality for proper access into the datacenter, and support capabilities that prevent data exfiltration inside sensitive networks.
- **Implement a solution to continuously scan** and detect ransomware, malware, and unauthorized encryption that does NOT rely on API calls, file extensions, or signatures for data Integrity.