(https://accuvise.com)

+1(tel:%205619108100)
(Https://outlook.office365.com/owa
561
910
8100
Book

(https://accuvise.com/in-the-news/)

What To Expect From A Security Assessment

In today's business climate, cyberspace is the new battlefield. It's only a matter of time before your company falls victim to a data security breach. Virtually anything can be attacked....

June 6, 2020 From Our Experts (https://accuvise.com/category/feature-news/)

When it comes to your private equity backed SMB, ask these security questions:

- How are you protecting your company assets?
- Are your user credentials safe?
- Can you encrypt and protect sensitive data regardless of where it lives?
- Can you centrally manage threats with the capacity to automatically mediate exposure?
- Do you have the ability to deploy a Zero Trust network (https://accuvise.com/what-is-the-zero-trust-network-philosophy/)?

If you've come back with a resounding "no", then you're setting yourself up for a malicious cyberattack. This is something that not only attacks the big guys. In fact, 46% of SMBs have been victims, and 73% have paid a ransom. And the average cost of an SMB data breach is $120k. If you are still not convinced, 62% of businesses lack the in-house skills to deal with security issues.

Will you be one of these statistics?

Your private equity firm (https://accuvise.com/new-microsoft-hack-hits-private-equity-firms-in-million-dollar-heist-heres-how-it-happened/) relies on its reputation as knowledgeable investment experts. The last thing is to admit is that it experienced a sophisticated ransomware attack, which has far-reaching consequences in terms of monetary and reputational losses.

So herein lies the question:

Are your portfolio companies safe? Have you performed any strategic planning for your company's security posture? Consider the ramifications if your servers, website, cloud tenet, client contact details, partner documents, trade secrets, or customer credit card data are compromised.

A security assessment is order. Here is what to expect.

Refocus on your assets' protection with a security assessment

Consider this: In a recent 2018 study, cybercrime generates more than 1.5 trillion dollars in illicit profits acquired, laundered, spent, and reinvested by cybercriminals. They are no longer "hoodies in bedrooms": these criminals belong to highly refined ecosystems after monetary gain and information that leads to economic damage, always looking for bigger targets.

Today, data is circling globally, and even more so when your employees are in the cloud. If it is not evaluated, this becomes a serious risk. It is your job to understand and tackle the economic environment that exists on this worldwide scale.

Also Read
Defining Digital Transformation

(https://accuvise.com/defining-digital-transformation/)
This is where a security assessment comes in. The assessment will help you to unify licensing, leverage your existing tools, and weave everything together to develop real protection for modern technology.

As part of security technology in business, there are the discovery phase and current state assessment. Using Information Security (InfoSec) experts, the security assessment is an excellent way to increase your understanding of your company's vulnerabilities and how to address them.

The discovery stage identifies the target network segment. This includes all active device addresses and their associated Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and other network services accessible from outside the internal network. Sniffers — in charge of monitoring and capturing data packets passing through a network — collect network traffic for parsing and analysis involving active host identification and authentication credentials. While used by network and system administrators to monitor and troubleshoot network traffic, attackers also use sniffers to capture data packets for accessing passwords, account details, and other confidential information.

The current state assessment identifies the various elements of your security program to ensure its able to protect your business. It is a sort of "How are we doing?" for your security controls. The elements include your hardware, software, cloud, personnel to support the operation, and the general IT in place. Every element is examined if it is functioning properly, requires an overhaul, or if replacement is in order.

Feeling threatened and vulnerable

Your InfoSec team will then perform threat and vulnerability identification and evaluation. You want to identify vulnerabilities, that is, some exploitations that permit any threats to breach your security and cause harm to your assets.

Also Read
It's Time To Break The Final Barrier To Digital Transformation

(https://accuvise.com/its-time-to-break-the-final-barrier-to-digital-transformation/)
Vulnerabilities can be physical or software-based whereby there are issues in areas such as:

- legacy technology that is often overlooked.
- excessive access permissions.
- personnel carelessness.

- insufficient training.
- or any combination of these four.

Once completed, risks are assigned based on a formula that assigns values of high, medium, or low risk, including cost estimates for each risk.

Down the road: What to do next

The final step institutes the recommendations and road mapping for remediation. Your security roadmap should integrate strategic planning on how to manage staff and budgetary resources. When it comes to your road map, just having a group of security experts is not enough. It should be forward-looking for a period of two to five years, and consider your company direction, market fluctuations, and the threat environment. As time progresses and threats evolve, you make revisions to your posture with confidence that you have the infrastructure to adapt.

Change your course of action

You've taken your security assessment on board and have your road map in place. Your next course of action is to incorporate that road map into digital transformation (https://accuvise.com/how-digital-transformation-is-driving-customer-experience/) by using people, process, and technology to achieve the desired transformation.

Free Consultation (Https://outlook.office365.com/owa/calendar/Accuvise1@Accuvise.com/bookings/)

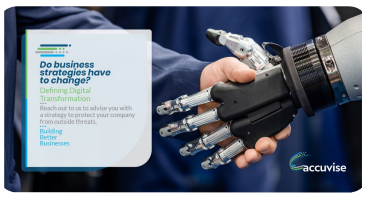
(Https://outlook.office365.com/owa

Book

Accuvise (https://accuvise.com/)

(https://accuvise.com/new-microsoft-h

(https://accuvise.com/what-is-the-zero

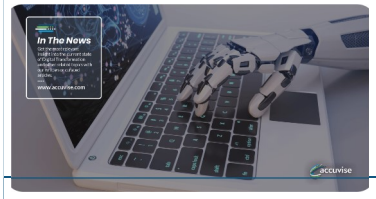


(https://accuvise.com/defining-digital-transformation/)

Defining Digital Transformation (https://accuvise.com/defining-digital-transformation/)

(https://accuvise.com/microsoft-takes-action-against-covid-19-related-cybercrime/)

Microsoft takes action against COVID-19-related cybercrime (https://accuvise.com/microsoft-takes-action-against-covid-19-related-cybercrime/)



(https://accuvise.com/its-time-to-break-the-final-barrier-to-digital-transformation/)

It's Time To Break The Final Barrier To Digital Transformation (https://accuvise.com/its-time-to-break-the-final-barrier-to-digital-transformation/)

A Fully BYOD Environment: Can it Be Secure? (https://accuvise.com/a-fully-byod-environment-can-it-be-secure/)

Russian Criminal Group Finds New Target: Americans Working at Home (https://accuvise.com/russian-criminal-group-finds-new-target-americans-working-at-home/)

Twitter Takes Down Over 32,000 Nation State Accounts Involved in Disinformation Campaigns (https://accuvise.com/twitter-takes-down-over-32000-nation-state-accounts-involved-in-disinformation-campaigns/)

Book (Https://outlook.office365.com/owa

Categories

Select Category

See All News
(Https://accuvise.com/archive)

Accuvise

+1 561 910 8100(tel:%205619108100)

301 E. Yamato Rd, Suite #3110 Boca Raton, FL 33431

(https://www.facebook.com/accuvise)

(https://www.linkedin.com/company/accuvise)


(https://www.instagram.com/accuvise/)


Book
(Https://outlook.office365.com/owa


(https://twitter.com/accuvise)