Castellum Labs

WHITE PAPER 2021

Security Awareness. What to Focus on?

Castellum Labs

WHITE PAPER 2021

Employees' "Action and Response" in IT and cyber world, knowingly or else unknowingly, can either protect organization's information and assets or else can wreck a havoc on security. Most organizations pay an exceptional attention to adoption of 'tools and technologies' to protect themselves against potential threats in the wild world of IT, but fail miserably, when it comes to equipping their employees with knowledge about 'threat', 'security precautions' & 'damage their response or lack of response could cause'.

This happens despite the fact that almost every organization arranges for some basic training on security awareness for their employees one or other time.

More than 60% of events are non-hacking related, and, are result of employee behaviors!

I believe most of the Indian companies, do not have requisite incident response models in place. Wipro probably is no exception, and, has just got caught into the midst of a breach, which happens to be reported by one of the well regarded and listened to security expert.

- Kreb reported a potential breach of Wipro, where its systems were compromised and then used for launching an attack on its own customers
- When Kreb asked Wipro some tough questions, about the reported/speculated breach, he got less that satisfactory and somewhat muddled response

Castellum Labs

WHITE PAPER 2021

What Employees Need to be Aware of...!

Employees in org need to be aware of certain scenarios and situations, in which, their actions should be based on their knowledge and judgement. Here is a list of things "All Employees" should be de nitely aware of:

- Using discretion in opening a document, which came from a mail ID out of their corporate domain
- Paying attention to a URL flagged as dangerous by either the search tool or by filtering tool deployed within enterprise
- Not clicking on a URL which came in embedded within a mail from an external source, unless it is a well known one
- Not turning off their scans at endpoint and not disabling the endpoint agent of whatever security products are installed
- Avoid getting trapped into social conversations, which lead to something related to work or profession without clear reason
- Stay away from posting any corporate content on any social or professional network without explicit permission of company
- Avoid using any external or cloud based backup tools/platforms to take back of their endpoint data without explicit permission
- Copying anything to removable media only when organization allows that specific content to be copied to such media
- Sending mails to external sources with company related information and being aware about what is allowed and what is not
- Good understanding of confidentiality policy of company and knowing how to respect and adhere to it
- Understanding threat vectors such as fishing, social engineering, viruses, malware and keeping themselves update the risk they pose
- Taking precautions in doing a login to corporate network from external networks and internet connections
- Understanding printing policy of the organization and adhering to the norms of using and destroying the printed copies of confidential material

- Knowing internet policies of organization, and, adhering to the type of sites which one visits during his presence in office
- Observing anomaly in the behavior of an external application, which employee use, and reporting it to internal management

Some or all of these are commonly known things and one would presume that all employees would already know it. 'True' and 'Not True'. The issues is not about employees knowing it. The issue is about employees being aware of the risk it poses, when they are not careful in 'Actioning and Responding' to one of the above mentioned scenarios.

"1,200 respondents surveyed for the report 40 percent of Gen Y respondents are likely to pick up a USB storage device found in public, compared to just 9 percent of Baby Boomers"

Measures to be Taken

Organizations need to think about the 'security awareness' differently than what they think about training. Security awareness in employees need to be done at much deeper level than a usual training on domain or any other managerial skill. Here are some things, which organizations should do.

Security Aware Program... Not a Training!

Security awareness is a program and not a training. Training is only one element of an overall security awareness program. Design a security awareness program which makes sense for your kind of organization, given the segment and environ you operate in. The program should have multitude of recurring activities, along regular training on security. Frequency and element of this program should be in alignment to threats and exposure your company is subjected to.

Sign up for Security Content... Third Party!

Arrange for regular security awareness and security news content, by signing up with some third party security vendor. This content should be dispatched to the employees on a regular basis with a feedback on, 'if employee read it'.

An aware employee is secure.

And, he makes the company secure!

Arrange for Security Awareness Assessment... Every Quarter!

Humans are capable of an incredible memory, and, then they are capable of 'legendary loss of memory', when it comes to non-contextual and non-interest topics and areas. Security awareness is such an area. People are likely to know stuff, but, still forget about taking precaution when it comes to taking an action or responding to a situation.

One of the most effective cure for this, is to conduct regular security awareness assessment and surveys. Keep it quarterly, and make it mandatory.

To make it even more effective, design certifications on security awareness, and, have people take the certifications and display them on their desk.

Make Security a Culture... Protection a Habit!

People in organization are more likely to 'do the correct thing', based on their security awareness, if they adopt it culturally. People place significance on some aspect of their work environment when everyone in the group is sincere about it. Inculcate a culture of being secure in your organization, and, let people take pride in it. The spread of this culture will ensure people intrinsically do the right thing and stay secure.

Have Security Expert Talk to People... Really!

A lot of time, people have a completely different sense of understanding and agreement, when a domain expert, which comes from outside world, is talking to them. Ask a security expert come to your organization and have him deliver a speech of perils of not adopting secure ways of working.

Key Services Areas

Application Security

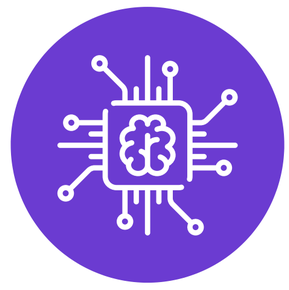
Managed AppSec Programs

Cloud Security

Cloud Security Design & Governance

SOC Monitoring

Managed Detection and Response



Threat Intelligence

Contextual Threat Intel & Hunting

Our Technology Platforms

appFORT

Continuous Application Security

watchOUT

Darkweb Monitoring

threatNIXD

Next Gen SOC Monitoring

Continuous Unified View of your Cyber Security

Get in touch with us to know more on our Cyber Security offerings

WHITE PAPER 2021

Castellum Labs

+91 97009 70397

info@castellumlabs.com

www.castellumlabs.com