Castellum Labs

WHITE PAPER 2021

Incident Response. Missing?

Recent Wipro fiasco on Breach reported by noted security researcher, Brian Krebs, is a study in either lacking incident response, or else, a mismanaged (or shall I use the word as muddled) incident response.

For the uninitiated...

- 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

Here are the links to Kreb's article...

https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

https://krebsonsecurity.com/2019/04/how-not-to-acknowledge-a-data-breach/

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.

Here are my observations, on the incident, and, its response cycle...

(most of these are modeled on what has been in media, and, Kreb's two articles on his popular blog ***https://krebsonsecurity.com/***)

COO Answering Questions on a Breach. Really ?

In Brian's report, he mentioned that Bhanu Ballapuram, COO of Wipro has answered most of his questions, during a quarterly call and post that, to media. Not sure, what a COO is doing, answering the pointed, objective and somewhat poignant questions of a top notch security expert. Where is the CISO?

Irrespective of preparations and data/facts support, a CxO, who is not CISO is least likely to be the right person to answer questions, posed by a security expert, who has in fact found and reported a breach.

If the CISO does not have a seat in Q call, and or, if he does not have the organizational clout and maturity to deal with media, to respond to media questions (specifically from a security expert), then, we are looking at a situation, where organization has either not realized the right person for the job, or else, has not placed requisite significance on this role, to be able to withstand a storm, which is usual after a reported breach.

First Response, "Defensive Posture"

Unlike what one would see in many of the enterprises' media handling, cyber security media handling is different. Default response in many of the events (specially the negative ones), in most of organizations is modeled around two factors.

- Negate the event (don't accept it)
- Downplay the significance (not much happened)

This may work in some of the usual corporate related incidents and events, but, would mostly lead to an embarrassment in case of a security breach reported by a media. Defensive posture does not work in case of cyber security incident (specially the breach), because of two factors.

- Cyber Security media is different, and, has experts at hands
- Market (and media) does not respond well to default denial model

First set of responses, by organization in this case, is reported as denial or downplay of the event/incident. One needs to remember, that, in this case, media run by a security expert, has brought an issue to notice of company, and, has not made simple accusatory comments, based on random speculations. This kind of reporting has efforts, intentions and most of all substance, and, can not be dealt with usual "denial standardized response model"

Castellum Labs

WHITE PAPER 2021

Several Days, for "Investigation"?

On the questions of "nature of breach" and its detection and knowledge status within, Wipro responded, "it would need several days, to establish the breach facts and then present an official stand".

Any organization worth their monitoring and detection and response ability, should be able to establish the facts of a given incident (specifically a breach), within hours, not days, not weeks. Asking for several days, to establish the basic facts about a reported breach/incident is analogous to "We don't have a clue". I am sure, Wipro has top notch detection & response tech and model at their disposal, but, does that have an equally well done and well aligned incident model and incident management model, to go along.

The fact is, if your SOC/Detection-and-Response systems and processes do not give you an ability to find out the details of a reported incident/breach, within hours, then, "they are not worth the dime"

Preparedness, "Lack of it"

As reported later by Wipro, that incident was largely a phishing originated, and, mostly a contained one, if that is true, why a well prepared response was not in ready state, for a Q call and for rest of media follow ups and questions.

Post a security incident, an organization has to be ready with all data and all supporting evidence, for many forums, irrespective of the fact if a question will be raised or not. Reading statement from a written report or a standard PR response of the company, is not preparation.

In cases of a breach, a well meaning, and a well defined response to all stakeholders, media being one of them, is needed. And, it is needed right after incident has taken place, not after some one has detected it, and, has placed you on a chopping board, through series of probing questions.

Updated Signature for an IoC, "That can't be a response"

What has been mentioned in the reported article by Brian Kreb, is, "Wipro confirmed that it has received an updated signature for a zero day vulnerability for its endpoint. And, that has been pushed all around, to all endpoints. That cannot be a response, to a breach, which has actually led to a compromised state of systems, specifically ones, which are concerned with customers.

The key questions here:

- Is that zero day established and recognized by experts or simply an explanation provided by your endpoint protection vendor?
- Even with a zero day, secondary security measures should kick in, and, should stop any form of infiltration beyond a specific endpoint or cluster of endpoint
- Why updated signature and its roll out is being dished out as a response? That is as basic, as hygiene reinforcements?
- Where is the part of response, which talks about scope of breach, its exact occurrence causes and its real impact on customer systems
- And, where is the part of response, which talks about operational model and operational process which failed, to detect and respond to incident in time, to prevent the compromise

Castellum Labs

WHITE PAPER 2021

What is "Security Eco-System" of India doing?

While Wipro is dealing with the aftermath of a muddles incident/breach response, a bigger question is about "Bigger Security Community of India". What exactly is the role of many security organizations and communities, which are active in India. Do they have a role to play, when a major services player of Indian IT industry, gets into the midst of such a breach?

- Has there been a support response by any security groups?
- Is there a coordinated model between services industry and security groups, when such a breach takes place, which can threaten wider interest of services industry?
- Are there any mandated reviews and discussions by governmental agencies/bodies when an incident/breach of this nature takes place, and, is being talked about worldwide?

While time will wither the storm, Wipro would still be staring in face of awkwardness, in coming days and months. If not the customer/revenue loss, such muddled response, would surely lead to reputation loss and also "higher cost of damage control".

A lot of services industry is already blamed to be porous and less than secure, from India. Companies such as Wipro, need to be establishing benchmark, for security, for rest of the community in India.

Castellum Labs

+91 97009 70397 info@castellumalbs.com www.castellumlabs.com

WHITE PAPER 2021