Meeting notes with

the Chief Information Security Officer (CISO)

This meeting aimed to investigate a security alert and understand a bit more the situation. The meeting was led by Bill Tench, CSIRT Manager at TechMaster.

Q: Did you observe any strange behavior on your systems so far?

A: Before contracting with you to monitor the security of our IT 2 years, we observed different kind of situations but since the last incident you managed, nothing has been noticed by our teams.

Q: Could you tell me more about the server “dmz-web”?

A: This server is part of our DMZ. A web server is running on it and exposes a web portal for our suppliers to submit the invoices for instance so our financial department can process them.

Q: Is your e-commerce website hosted on the DMZ as well ?

A: Of course not ! The e-commerce website is hosted in a cloud provider to ensure the highest SLA possible. The DMZ is only for business purposes.

Q: By compromising the DMZ web server, what kind of sensitive information an adversary could access to ?

A: As I told you, the invoices of our suppliers as well as the purchase orders. It’s a lot of financial duties. This is not really sensitive to be honest but it could be annoying to see these data leaked on a public place.

Q: Would you have a database with all your customers ?

A: Yes, we have a CRM but to be honest, this is a different internal server that hosts this internal server and I don’t think it could be possible from the DMZ to get access to this data. Anyway this data is encrypted.

Q: Could you enumerate the different cyber security measures implemented to know how properly managed this alert ?

A: Sure. First all our employees have an Antivirus deployed on their computer except the developers and system administrators because it was consuming too many resources. We also deployed a NIDS on the router to inspect the network traffic 5 years ago. But the administrator who was in charge of the NIDS left 3 years ago unfortunately and we had no budget to hire a new one. But we had the budget to contract with you and you put in place a SIEM monitoring and you are currently putting in place a proxy !

Q: What about you firewall policy ?

A: Good point ! We have a firewall configured on the router to block unwanted incoming traffic. The only incoming flow allowed is forwarded to the DMZ.

Q: Thanks for your time. Do you see anything else to add before we start investigating ?

A: I think I told you everything. Please keep me informed about your investigations and I would be very interesting to get your opinion about the security of the company and what we should improve and on what we should focus on first.