Learning cyber security from mistakes

SecurWHAT ?!

Book sample

Jean-Luc Dupont

I'm Jean-Luc Dupont and I do cyber-security. My approach is practical. I did not learn this profession only through studies or advanced education. No, I mainly learned it through my mistakes.

This book contains dozens of short anecdotes along with real-life lessons that can be applied in your day-to-day journey as a security professional. Many of you will be able to relate to those funny, sad, or sometimes even frightening events. Some are good. Some are bad. I learned from them all.

The stories you're about to read are all true and I lived through almost all of them personally. You may call this a book of mistakes.

I call them experience.

Contents

22. Hail to the King, baby!

Jeremy and I were installing firewalls and switches for a small bank. By installing, I also mean physical installation. Those switches were Cisco 6500. They were big, heavy babies, and you needed two people to rack them. You often ended up with bloody hands after the installation, sweating profusely. This installation was no exception. We just finished the physical part, and now could work on the logical configuration.

“Phew!” sighed Jeremy as he leaned on the wall.

“Jeremy! No!” I screamed in horror.

Too late. Jeremy accidentally pushed that big red emergency stop button. All the equipment in the room became instantly silent.

The bank CIO rushed inside the server room, “What have you done? What have you done?”

“Well, we, uh, that button, and, uh, stopped everything,” I mumbled.

“That emergency stop button was really not well positioned,” asserted Jeremy.

It was the first time I had worked with Jeremy. My coworkers told me he was never stressed. He would never lose his cool.

“But you don’t understand. You just shut down our main server. All our branches can’t work anymore,” gasped the CIO.

“Well, you just need to power them back up,” assured Jeremy.

“Those mainframes are ancient. They don’t start up like this, especially if they’ve not been shut down properly. It will take three full days for them to be operational again,” whimpered the CIO.

Jeremy responded, “Ok, today is Friday. I say you shut down your branches from now on until Monday. As for us, we will come back on Tuesday, when everything is back in order. I really suggest you put some protection on that emergency button, or you move it somewhere else.”

And we left with the CIO in disbelief. An army of technicians was already working in the server room, powering up those systems one by one.

“You’re really someone,” I told Jeremy outside.

For some reason, the customer did not want us to go back to his server room that Tuesday. Or any other day for that matter. And from that moment onward, everyone started calling Jeremy "the King."

Lesson learned: Don't put all your eggs in the same basket. If you have critical systems, put them in two different buildings with a replication system.

Lesson learned: Critical equipment should be powered by two totally independent power sources.

Lesson learned: If you have an emergency shut off system, physical or logical, make sure you cannot trigger it accidentally.