RSA Conference 2018

NOW MATTERS

Peer2Peer

Role playing an incident, except it's fun

P2P2-T07: Dungeons and Data, Let's Role Play an Incident

Josh Bressers, Head of Product Security, Elastic

At RSA Conference 2018 I had the pleasure of holding the same session twice. Normally this would mean doing the same basic thing the second time, but my session was rather unique: I held a role-playing event that was very heavy on randomness. I've participated in and hosted security role playing events in the past and most of them were a bit on the dull side. My idea for this year was to spice things up a bit. We role played an incident, but everything was random. There were dice and I rolled against tables to decide what happened, why it happened, and to who. Both of my sessions were completely different as one would expect, but there were a couple of really interesting themes that carried over between them.

All of the content I used can be found here: https://drive.google.com/open?id=1lUSi7HqDa-hKWicfDxpBMLG-qB1UrtsU

I plan to expand this in the future and host similar sessions, as I do I'll be sure to update the content to add in new ideas and take out things that don't exactly work. As the saying goes, patches welcome. Feel free to let me know if you have ideas or content you'd like to contribute.

Firstly, if you've ever role played with your friends it's usually a small group, five or six people. At RSAC a Peer2Peer room holds 30 people. 30 people! That's a crazy number for role playing. It also meant I had to give 30 people dice and create 30 character sheets. It was far more work than I thought it would be, but in the end, it was worth it.

I asked the players in the room how many had played games like Dungeons and Dragons in the past and about half had. It certainly wasn't a requirement to playing and everyone caught on quickly which was great. I would suggest whoever runs the game have some experience as a game master. The most important thing when you're putting something like this together is being flexible and thinking fast. The game can take crazy turns and players can do almost anything. That's also part of the fun. I suspect I had more fun than the players did during the sessions.

To set things up everyone got a character sheet and three dice. I just used 6-sided dice as they were very inexpensive (it turns out trying to buy a dice set for thirty people is not cheap). The game was meant to be fun, and due to the random nature of events unfolding everyone was warned that things won't always make sense, but they should go with it. A few people complained that having a middle eastern and western government attacking at the same time was ridiculous, but that's just how to dice roll.

The basic idea is every person in the room has a character sheet that determines what they do for a fictional company. This was interesting because it made people step outside of their typical comfort zone and think like someone else. The people who were in charge of PR learned a lot about what they should or shouldn't do, a thought process that was never a second thought before role playing the part. Making people step into the shoes of someone else ended up being the most enlightening and important aspect of this exercise. I didn't expect so many people to comment on how much they learned by playing as a lawyer, marketing person, and even CEO. I think having non- security people play the role of security professionals could be equally powerful in the other direction.

In a typical role-playing session, you have a round where everyone takes a turn. With thirty people one round would probably take longer than we had for the entire session. To deal with this we had timed rounds which turned out to be perfect. Every five minutes a new finding was uncovered which represented a round. Anyone could talk anytime they wanted. Of course, some people didn't talk much which is inevitable in a group of thirty.

The session kicked off with an email to the CEO that claimed if a ransom wasn't paid they were going to leak their customer data to the press. The most surprising theme from both sessions was the first instinct everyone had was to try and pay the ransom. Even after I assured them that as the game master there was no way I'm going to let them pay the ransom they kept trying to get it done. I have a suspicion this is just the human condition to try to find the quick way out of a stressful situation.

Once the game started it was up to the CEO to kick things off. There was a bit of confusion at the start as it's hard to know who to talk to. This mirrors real life in a lot of ways. When there is an incident it's not always clear who to speak to first. The two sessions ended up with the CEO talking to the CISO who then started to ask questions of the security staff.

The event continued to unfold and the teams did their best to understand and contain. The participants quickly realized how much work it can be to juggle the tasks around understanding what's happening as well as dealing with external communications with the press and the board of directors. Even dealing with each other could be tricky where the lawyers and PR groups were demanding answers.

Both groups accidentally leaked too many details to the press which of course resulted in some rather funny results from the other players. The person who was the head of PR made an important observation at the very end of the game that they should have sent out some sort of note to everyone telling them not to talk to the press. This is the sort of thing I don't think a security professional would generally think about if they weren't put in a role-playing position such as this.

One group wrongly identified one of the other players as an insider threat. The game wasn't setup with an insider as a threat but I plan to add this in future versions. The best part of not having an insider threat was watching the player being blamed try to defend themselves. They did manage to convince everyone else they weren't the attacker.

One of the best aspects of using dice and randomness for a role-playing incident like this was when players would fail. Everyone has certain skills and the dice are rolled to see if something works. If they roll below the skill number, it works. If they roll above they fail, but they don't know they failed. An example is when a web server was found to be compromised one of the players tried to patch and clean it up. They failed the roll but thought they accomplished their task. The players know the roll was failed and have to continue playing the game knowing it failed, but the characters they play in the game don't

know it failed. Everyone understood this and played along perfectly. This is a bit like real life where during a crisis we often make mistakes and don't realize what we've done.

On a whole I had more fun running these two sessions than I could have imagined. The people were great, we learned a lot, we laughed a lot, and everyone had ideas on how to improve the game in the future. I'm a huge fan of gamification and I think what this session really made me realize is gamification by itself isn't what's useful, what's useful is making sure everyone is engaged because they're having fun. Something as simple as rolling dice can keep everyone more engaged since you're writing the story instead of just an observer in someone else's story.

I'm really looking forward to expanding the game in the future and I can't wait to run more sessions. I highly encourage anyone looking to expand awareness and empathy of their teams to give this a try. It was a great use of time.