Things You Can Do to Make Security Worse in Your Network - Ignite Style by Jack Rhysider

i used chat gpt voxscript to get this coz its great, but its 7+ years old and he stutters allot and didn't have allot of skill in making videos yet

---

Introduction

Things you can do to make security worse in your network. Why would you want to do this? Well, I'm a security professional and I've seen lots of networks all over the world: schools, hospitals, retail, high-rise, manufacturing, public utilities, even state agencies. And I often assess these networks for security to, you know, give improvements for their security.

What I keep seeing is that organizations spend time, money, and resources to make their own security worse. Security is challenging, okay, I get it. It's not for the lazy. But these organizations are going out of their way to be insecure. That is, they could be doing nothing at all and they would be better off. It's almost like it's a goal to make it less secure. Maybe this is an industry trend that nobody's talking about.

So here's the thing, if you work for an organization that wants to make your network less secure, this is for you. I'm going to go over five ways you can make your network insecure.

1. Change Your Default Passwords to Something Shorter

Number one, change your default passwords to something shorter. This makes about as much sense as Spongebob taking a swim at the bottom of the sea. You may have heard from your boss or somewhere else that you should change your default password. Well, so you go ahead and you make the effort and go ahead and do it and when you choose one, you just choose ABC or pass. Doing this, like, you probably would have been better if you just left it as your default because you definitely made security worse in your network.

2. Make Security Awareness Training Programs Boring

Alright, so now you should also make security awareness training programs boring. You're going to spend thousands of dollars developing a security awareness training program and then you're going to take everyone in your organization out of their busy day and make them attend this. And in order for it to be as what a waste of time and money as possible, you want to make it as boring as possible. That is, don't make it real meaningful or useful or exciting to anyone that attends it. And another cool trick is easy to use the same exact security awareness training program for everyone in the organization. Doesn't matter how a technologically advanced you are or beginner you are, use the same program and bow people will find it just as useless.

3. Make Security Policies Hard to Find

Make security policies hard to find. These are the things that tell you what you can or can't do in a network. When you write them, you're going to spend hours doing it and editing it and then getting a leadership approval, maybe even lawyer approval. And when you're done, hide it at the bottom of SharePoint in an internal website then nobody ever goes to and then put a title on it that nobody's ever going to think to search for to find your security policy. Your goal here is to take all that time and energy and effort you made, you used to make this security policy and make it as wasted as possible by hiding it as away from everyone is that you can. You don't want anyone to know what's in it, where it is, or who to call when there's an incident.

4. Do Nothing with the Results from a Security Assessment

Okay, you can try this, do nothing with the results from a security assessment. Now you might be thinking that's just being lazy, how does that going out of my way to be less secure? Well, somebody had to agree to a security assessment and then somebody had to approve the budget for a security assessment and these things sometimes cost ten thousand, thirty thousand dollars. And then when the security assessment results come in, see, you just do nothing about it, let it fall right on the floor, take a step back, look the other way, do nothing with this, with the security assessment results. It's like burning money. And when you have a failing security assessment and you do nothing about it, it's like watching your school kids fail in school and then you, you know, still give them a handsome reward and do nothing about it.

5. Your Security Team Should Act Superior to All Other Teams

Alright, lastly, your security team should act superior to all other teams. Security professionals love laughing and making fun of anyone who fails at security and they think they have security all figured out and they cannot understand why nobody else can do this right and they act like this guy sometimes. And when the security team acts like this, it actually does more harm than good. So if that's the goal of your organization, you want to make security worse, then by all means, let's start. You should start yelling at your users, slap them around when they don't follow the security policy that they could not find and they don't even know it exists. Make them feel like aim for that kind of thing. You should criticize, ridicule, and yell at any of your users that didn't pay attention and that boring as security awareness training program that you made them go through.

Conclusion

Okay, so that's some real things you can do to make security worse in your network if that's your goal. Thanks for your time. Find me online at TunnelsUp.com or on Twitter at TunnelsUp. Let me hear what your thoughts are.

Revision #2
Created 19 July 2023 08:10:47 by naruzkurai
Updated 19 July 2023 08:39:59 by naruzkurai