Kaspersky was banned

In this episode of the DarkBox Archive, Andrew and Josh discuss the US government’s ban on Kaspersky cybersecurity products. They cover the reasons behind the ban, including concerns about potential exploitation by Russian intelligence agencies, and its implications for users and businesses. For more information, visit darkboxsecurity.com and join their Discord community.

Cybersecurity Incident Response

In this episode of the DarkBox Archive, Andrew, Thai, and Josh explore incident response in cybersecurity. They define it as a structured approach to managing security breaches, aiming to limit damage and reduce recovery time. Key steps include Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. They emphasize the importance of having a plan, effective detection, damage control, threat removal, careful recovery, and post-incident analysis. Best practices include updating plans, fostering cybersecurity awareness, using automated tools, and clear communication protocols. Visit darkboxsecurity.com for more resources and join their community on Discord.

The Dangers of Phishing

We discuss the dangers of phishing and give ways to protect yourself. Phishing has evolved overtime and has become more difficult to detect. It is considered the number one way companies get breached.

Why cybersecurity is important

Join our Discord channel here.

Our first episode of our cybersecurity podcast. We discuss why cybersecurity is so important and give some advice on how to improve your cybersecurity if you are a business or for personal life.

Top 5 reasons to do a penetration test

Penetration testing, also known as pen tests, are authorized attacks against your computer systems to look for any security vulnerabilities. Here are the top 5 reasons on why you should perform a pen test:

1. Identify vulnerabilities: A penetration test can reveal weaknesses in an organization's security infrastructure that could be exploited by attackers.

2. Compliance: Many industries have regulations that require regular penetration testing to demonstrate compliance with security standards.

3. Improve incident response: Understanding how an attacker might penetrate a network can help an organization develop better incident response plans.

4. Prioritize security investments: By

identifying vulnerabilities, a penetration test can help an organization prioritize which security measures to implement first.

5. Improve employee awareness: A penetration test can help raise awareness among employees about the importance of security and the potential consequences of security breaches.