NOTICEBORED

Board agenda

Malware (malicious software)

Introduction

Please contemplate the questions, mark the scales at the appropriate positions and prepare to discuss malware at the next meeting.

1. Are we keeping pace with the escalating malware threat?

Malicious software has come a long way since the simple viruses and worms of the 1970's and 80's. Today's malware is: used for criminal purposes; actively evading antivirus software; infecting and harming almost all organizations; stealing valuable industrial secrets, intellectual property, passwords and personal information, or encrypting it for extortion (ransomware); draining corporate bank accounts (bank Trojans); sometimes used for military purposes, staying undetected for months or years, waiting to strike (APTs – Advanced Persistent Threats - multifunctional, deeply embedded malware, remotely controlled and remotely updateable); nasty stuff indeed!

We're backward | We're falling behind | We're ahead | We're cutting-edge

Notes:

2. Are we prepared to cope with a *major* malware incident?

Although malware incidents are commonplace, most – thankfully – are identified and resolved efficiently with minimal damage and costs. The increasing sophistication, variety and number of malware attacks, however, suggest that the preventive controls are failing, hence we should anticipate more frequent and/or more serious incidents … to the point that we may well need to invoke business continuity and disaster recovery arrangements. Are you confident that we are ready for that fateful day if and when it comes?

No, not at all | A little | Somewhat | Yes, absolutely

Notes:

For more information

Please check the intranet *Security Zone* or contact the CISO/Information Security.

Copyright © 2016 IsecT Ltd.