BH Consulting

Helping you piece IT together

Computer Viruses Threats & Solutions

Disclaimer:
BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. Computer Virus Threats and Solutions 4

2. Contact Us 7

1. Computer Virus Threats and Solutions

Once the realm of IT Security Professionals, computer viruses are now becoming an issue and concern for business people. Recent major computer virus outbreaks such as the Sober, Mydoom and Sobig viruses have caused many hours of downtime for companies throughout Ireland and the world. The resulting chaos meant many companies' computer systems were offline until the infected systems were restored. Productivity was lost, projects were delayed, important deadlines missed and management time diverted to deal with frustrated customers and/or business partners.

Computer viruses are becoming more and more sophisticated and employ many different methods of spreading. While email has been the primary method for the spread of these recent computer viruses, it is not the only method. A computer virus can enter a network by CD, floppy disk, Internet download, file transfer and file sharing programs, or by remote users connecting directly to the corporate network with an infected PC. Once a computer virus gets into a network it can spread from computer to computer in multiple ways.

Given the numerous ways a computer virus can spread, how can a company ensure that its network is protected?

1. **Install Anti-Virus Software.**
   Ensure that reputable anti-virus software is installed on all computers. This should include all servers, PCs and laptops. If employees use computers at home for business use or to remotely access the network, these PCs should also have anti-virus software installed.

2. **Ensure that the anti-virus software is up to date.**
   Everyday new computer viruses are being released and it is essential that business is protected from these viruses by keeping the anti-virus software up to date. If possible, companies should look at policies whereby computers that do not have the most up to date anti-virus software installed are not allowed to connect to the network.

3. **Employ a firewall to protect networks.**
   As computer viruses can spread by means other than email, it is important that unwanted traffic is blocked from entering the network by using a firewall. Sensitive areas with a company's network should also be further segmented and protected using additional firewalls.

   For users that use computers for business away from the protection of the company's network, such as home PCs or laptops, a personal firewall should be installed to ensure the computer is protected.

4. **Filter all email traffic.**
   All incoming and outgoing email should be filtered for computer viruses. This filter should ideally be at the perimeter of the network to prevent computer viruses. Emails with certain file attachments commonly used by computer viruses to spread themselves, such as .EXE, .COM and .SCR files, should also be prevented from entering the network.

5. **Educate all users to be careful of suspicious e-mails.**
   Ensure that all users know to never open an email attachment they are not expecting. Even when the email is from a known source, caution should be exercised when opening attachments. Recent viruses have spread because they appear to be from addresses familiar to the user.

6. **Scan Internet Downloads.**
   Ensure that all files downloaded from the Internet are scanned for computer viruses before being used. Ideally this scanning should be done from one central point on the network to ensure that all files are properly scanned.

7. **Don't run programs of unknown origin.**
   It is important that a company establishes a trusted source for their software requirements. This is to ensure that all software installed within the company can be accounted for and that its sources can be confirmed to be legitimate. Apart from ensuring that the correct licensing agreements are in place, using a trusted supplier can help reduce the risk of software infected with a virus entering the company's network. All users should be educated to never run a computer program unless the source is known or has originated from a person or company that is trusted and has been authorised by those responsible for managing the company's network.

8. **Implement a vulnerability management program.**
   Most computer viruses and worms try to exploit bugs and vulnerabilities within the operating system and applications that companies use. New vulnerabilities are introduced into networks everyday, be that from installing new software and services, making changes to existing systems or simply from previously undiscovered vulnerabilities coming to light. It is important to regularly review your network and the applications running on it for new vulnerabilities. In accordance with your vulnerability management program, these vulnerabilities should be rated and prioritised regarding their criticality and the potential business impact they could have. Once this has been done, a plan on how to manage those vulnerabilities, either by patching, upgrading, or managing the vulnerability using tools such as firewalls or Intrusion Detection Systems should be put into place.

9. **Make regular backups of critical data.**
   It is important to ensure that regular copies of important files are kept either on removable media such as CD-ROM discs or tape to ensure a trusted source for data in the event that the network is infected with a computer virus. Not only will this ensure that important data is available in the event of a computer virus infecting the company's network, backups will also enable the company to restore systems to software that is known to be free from computer virus infection.

10. **Develop an Information Security Policy.**
    The creation and publication of an Information Security Policy is key to ensuring that information security receives the profile it requires in the organisation and is the first critical step in securing the company's systems and data. It is important that senior management support the Information Security Policy and that all users are made aware of their roles and responsibilities under this policy.

11. **Monitor logs and systems.**
    Regular monitoring of network and system logs can assist in the early identification of a computer virus infecting the network. Unusual traffic patterns or log entries could indicate that the network has been infected. As well as monitoring for suspicious traffic and events, it is important that logs for other devices are checked regularly to ensure that the network remains protected. Log files for the backups should be checked regularly to ensure that the backups succeeded, likewise the log files for anti-virus software deployed should be regularly checked to ensure that all PCs are running the latest version of the anti-virus software.

12. **Develop an Incident Response Plan.**
    Knowing what to do when a computer virus enters the network is critical to minimise the damage the virus may cause and to prevent it spreading further internally or externally to customers and suppliers. The incident response plan should outline the roles and responsibilities that people have in the event of a computer virus infecting the network. This plan should be drawn up and agreed between all relevant parties before an incident occurs. Remember, the worst time to develop a security incident response plan is in the middle of such an incident.

13. **Restrict end user access to systems**
    Where possible, end users should not be given administrative privileges to their workstations. Most computer viruses can only run in the context of the user that is logged into the system, i.e. they only have the same permissions as the user running the program. If that user has their access restricted, then the virus will be similarly restricted. Unfortunately many applications designed for the Windows platform require the end user to have such privileges; however these users should be the exception rather than the rule.

Computer viruses pose a very real and constant threat to every business. It is important that businesses recognise this threat and take the appropriate steps, such as the above, to reduce the likelihood and minimise the impact of being infected with a computer virus.

2. Contact Us

Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : **+353-(0)1-4404065**
Website : **http://www.bhconsulting.ie**
Email : **info@bhconsulting.ie**