Datasheet:

Dark Web

APH CyberProtect for Businesses

Ensuring the security of your business, data and IT systems are protected is the first step in eliminating the risks to your business from security threats and data breaches. Thankfully, there are different measures and systems that can be put in place to keep your business, data and IT systems secure.

What to be aware of

- Server and Network Firewalls
- Email Security and Anti-Spam
- Web Security
- Single Sign On
- Anti-Virus

WE IDENTIFY
COMPROMISES
Throughout your organization.
EMPLOYEE CREDENTIALS ARE A BEST SELLER ON THE DARK WEB
WE MONITOR
24/7/365
• Hidden chat rooms
• Private websites
• Peer-to-peer networks
• IRC (Internet relay chat) channels
• Social media platforms
• Black market sites
• 640,000+ botnets
WE REPORT
80,000+
Compromised emails daily.

46% of businesses and 26% of charities have been victimised towards breaches and attacks in the past 12 months. Phishing is considered to be the most disruptive types of attack that organisations face. Seeking information and guidance on cyber security you are more likely to be aware of data breaches and attempted threats to your business.

Phishing

Phishing is a highly effective and very common way for attackers to infiltrate a business's network. Would be attackers generally send a very convincing email to end users claiming to be a genuine service such as Microsoft Office 365 or a banking service. The victim of the attack is generally unaware of the attack and submits their credentials to a fraudulent website that looks just like the real thing. Now the attacker has the credentials to log on to the real service and can impersonate the end user and carry out a raft of further attacks compromising the businesses finances and reputation.

Despite the numerous security controls a business can have in place, anti-spam, firewalls, anti-virus, occasionally a phishing email can get through and at this point the next security control is vital, training.

Many small and medium business do not have the time or resource to provide training on Cyber Security. APH have a service that can provide training through the use of simulated Phishing attacks. APH can create campaigns that run on a periodic basis, weekly, monthly or quarterly that send users simulated Phishing emails mimicking various online services such as Office 365, online banking services, HMRC. If the user submits credentials, they are advised it was a test and and directed to a brief online training session on Phishing and Cyber Security. The campaigns are customisable for your business and can be configured to suit your requirements.

Reporting is provided to senior management to show the effectiveness of the campaigns.

Email Security Advice for Clients

What should I be looking out for?

Is the email a trusted source?
Review the "From" address - attackers often impersonate or "spoof" staff by using incorrect spelling of names or domains you may be familiar with or in contact with e.g. "@yourd0main.com". The display name may look familiar 'John Smith'. But does the underlying email look correct?

If the email appears to be internal, you can check this by double clicking on the display name on the email, this will reveal the senders' original address.

Review the subject of the mail
Attackers often try to include valid email information in the subject to trick the user into believing the email is legitimate, the best course of action is to check with your IT contact or APH.

Review the spelling and content of the mail
Attack emails often contain poor spelling and grammar.

- Ask - "Is this mail relevant to my job role?"
- Is the nature of the email related to your job?
- Does the mail refer to an action you didn't take?

Be vigilant of attachments
Attackers will often include a malicious file as an attachment to a phishing email.

DO NOT OPEN or interact with any attachments in strange or suspicious emails. Verify that:

- The sender is legitimate
- Content contains legitimate mail history
- Attached file is the one you have requested
- Attachment is the correct format

I'm not sure if the email's genuine, what do I do?
If you are not sure contact the sender directly by telephone.

I think my account is compromised, what do I do?
The best course of action would be to contact APH first. We can assist you through the process of resetting your accounts and re-securing them.

Monitoring for exposed credentials is important to make sure that your business is fully protected against attacks.

Unfortunately usernames and passwords are the most common method for logging onto services including corporate networks, social media sites, e-commerce and others. Usernames and passwords represent the key to the kingdom and to attackers. Criminals who know how to penetrate a company's defenses can easily steal thousands of credentials at a time.

HOW ARE CREDENTIALS COMPROMISED?

PHISHING
- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLES
- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING
- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACKS
- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

YOUR INFORMATION IS ALREADY EXPOSED

This information is used to compromise your corporate services such as: Office 365, payroll services, VPNs, remote desktops, banking, VOIP, ERP, CRM, social media access, ID Theft.

Introducing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organisations protect their business from perils on the dark web.

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

Making sure everyone is aware of the potential risks to credentials being compromised is an influencing factor which can help keep your business protected by potential threats. Making sure all staff are warned and trained is a way of making sure all your data is protected.

APH (North) Glencroft House, Vale Road,
Heaton Mersey, Stockport SK4 3QR t: +44
(0)161 442 2603
e: hello@aph.solutions