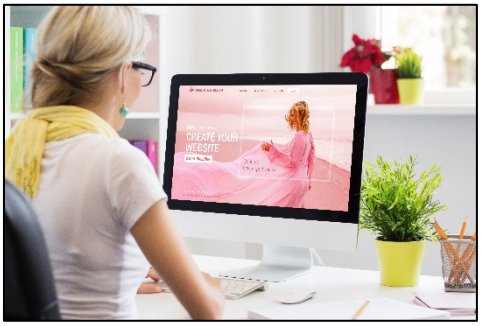
East Midlands Special Operations Unit

EMSOU CYBER SECURITY ARTICLE

Thursday 8th April 2021

This article has been written by EMSOU and seeks to promote good cyber security among businesses and the public. If you require any further assistance or guidance please contact the EMSOU Protect Team or your local Force Protect Team.

Todays Topics: Website Defacement



Times have certainly changed. Over the past couple of decades, more and more organisations have taken to advertising online, in order to establish their credibility as a legitimate business. A website that looks good and clearly communicates key messages, can dramatically affect the reputation and profitability of the enterprise.

This is why website defacement - or virtual graffiti as it is sometimes known – is so damaging. A hacker defaces a website by changing its appearance or content. Reasons for doing so, are usually borne out of the desire to embarrass the organisation or to promote alternative social or political views (known as hacktivism).

Other motives include:

- Personal enjoyment or the challenge to find and exploit system vulnerabilities.
- Redirecting visitors to commercial websites to make a profit or malicious sites to exploit targets.
- To steal customer data.

How Are Websites Defaced?

Typically, a hacker will make use of well-known web vulnerability tools to look for security weaknesses. This might include poor authentication methods, for example, allowing the hacker to bypass usernames and passwords. Alternatively, there might be poorly designed input fields that allow the hacker to enter malicious script. This script enables the attacker to:

- Raid the database that back ends the website - stealing your data.
- Plant harmful software on the visitor's device - not nice!

The attacker might also use a virtual private network (VPN) to hide their identity and will change your account details to prevent you logging into your own site. This makes it extremely difficult to remove unwanted alterations.

What To Do If My Website Is Defaced

If an attack takes place, it is always a good idea to:

- Replace the site with a maintenance page whilst the incident is investigated.
- Identify how the hacker was able to gain access.
- Inspect pages for any hidden malware left by the attacker.
- Inspect back-ups to ensure data integrity.
- Add compensating controls to prevent a reoccurrence.

- Implement a straight forward fix or roll back to a previously working state.

The severity of the attack will also influence the decision to inform relevant 3rd parties and key stakeholders. The exposure of customer data - for example - will most likely fall under GDPR legislation. As such, the data owner (you) must notify affected customers and the ICO as soon as it is reasonable to do so.

Alternatively, you may need to reach out to the public to limit the damage to your reputation and branding. It pays dividends, therefore, to plan your PR strategy well in advance. Who needs to be informed, by when and by what means? Ideally you want to be transparent and proactive about what has happened.

Finally, reporting the attack to Action Fraud is a good idea. Police cyber response teams can often offer exceptionally good advice for free.

I Use A Website Vendor – What Should I Do?

Most website vendors will explain the security standards their systems or products align to. These standards will invariably help the provider to:

- Identify security risks to their websites.
- Apply security controls to mitigate these risks.
- Asses the efficacy of such controls.
- Develop incident response plans to identify, contain, sanitise and restore services as well as prevent a reoccurrence.

When choosing a vendor, keep an eye out for

- Risk Management Frameworks: E.g. NIST RMF, OCTAVE, ISACA Risk IT Framework, ISO 31010:2009
- Cyber Security Frameworks E.g. PCI DSS, NIST SP 800-53 r5, ISO 27001:2017, CSA CMM, CIS Top 20
- Incident Response Frameworks E.g. SANS INSTITUTE, NIST SP 800-61, ISO 27035-2, CERT
- Evaluation criteria for software procurement or development. E.g. ITSEC, Common Criteria, Software Capability Maturity Model

These frameworks are widely considered best practice. However, you will also need to read your contract and service level agreement carefully as this will outline what actions the vendor will take and how quickly you can expect them to resolve the issue.

Wait . . .I Develop and Host My Own Site. What Can I Do?

Always pay close attention to:

- How the websites has been developed. Security must be built in from the get go. This means following well defined procedures for software development. See the Application Security Vulnerabilities Standard (ASVS) for the ultimate guide to secure web applications.
- Use strong unique passwords, 2 factor authentication and remove default log-in credentials to keep hackers out.
- Manage user accounts carefully. For example, remove users who have left the organisation or no longer require access. Administrator accounts, in particular, must be kept to an absolute minimum and should only have the privileges necessary to execute job responsibilities and no more.

- ± Install updates and patches on your website server or anything that affects the code used to develop the site.
- ± Use a web application firewall to flag and block malicious traffic.
- ± Use monitoring and detection tools (such as Tripwire) to track unauthorized changes to your website.
- ± Use a web vulnerability scanner and have your site pentested to check for exploitable loop holes. Many scanners will also check the site against the OWASP Top Ten. These are the most common security issues found online.
- ± Back up your site and any associated data regularly. Keep these backups separate and offline so restoration is viable.
- ± Train employees on incident response procedures for a range of different security incidents.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).