BULLET PROOF

10 POINT SECURITY CHECKLIST

A PRACTICAL ASSESSMENT FOR A 360^0 VIEW OF YOUR SECURITY READINESS

Completing this 10 point checklist will guide you through the simple steps you can take to stay ahead of the hackers and keep your data secure against costly data breaches.

A staggering 88% of UK companies suffered a data breach in the last year alone[1], and one in three companies report losing customers as a result of a data breach[2]. This makes cyber security a top priority for the whole of the UK economy. Gaining robust cyber defences has often had a reputation for being expensive, difficult to resource and a headache to manage. But it doesn't have to be this way. Bulletproof believe that strong security should be simple and effective for every organisation.

1 PENETRATION TESTING

Penetration testing is seen as the cornerstone of a cyber security defence strategy. It's where trained security researchers use all the tools and techniques of real-world hackers to simulate a cyber attack in a controlled and pre-defined manner. Key to penetration testing's value is the use of human insight and ingenuity to find flaws that automated scans would miss. This gives you the power to fix complex security weaknesses and so prevent data breaches.

Assessment Checklist

□ Conduct penetration testing at least once a year

□ Source the right test for my applications & infrastructure

□ Customise testing parameters to meet my security objectives

□ Outline a plan for re-testing and remediations based on test findings

□ Find a reputable third party with CREST and/or Tigerscheme certifications

□ Check report will contain both an executive summary and technical detail

> *"Without a penetration test, the first you'll know of a critical security weakness is when you're hacked."*

[1] https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html

[2] https://www.redseal.net/files/PDFs/RedSeal%20UK%20B2B%20Research%20SUMMARY_July2019.pdf

2 VA SCANNING

Vulnerability scans (or VA scans) are automated assessments that methodically search apps and infrastructure for publicly known security flaws. By assessing services, ports, applications, network devices, servers and other components, you can see where your organisation is vulnerable to attack. This allows you to fix security weaknesses before an opportunist hacker exploits them.

Assessment Checklist

- □ Schedule monthly VA scans to maintain security between penetration testing cycles
- □ Customise my scans to suit different infrastructure components and applications
- □ Keep my scan engine up to date to protect against the latest threats
- □ Perform additional ad hoc scans on new deployments/environments
- □ Use the report findings to create a remediation plan

“Monthly VA scanning is seen as the industry standard for a strong level of cyber security.”

3 CYBER ESSENTIALS

Cyber Essentials is a Government-backed certification, designed to help every organisation get the basics right. Certifying as Cyber Essentials or Cyber Essentials Plus helps demonstrate to potential customers a good commitment to cyber security. In addition to helping win new business, Cyber Essentials certification is also required for certain Government contracts.

Assessment Checklist

- □ Review implementation options to suit internal skills and resources
- □ Allocate budget and staff resource
- □ Undertake the technical assessments
- □ Remediate potential failures
- □ Complete questionnaire

“Cyber Essentials Plus is mandatory for NHS by 2021 and permits businesses to accept MoD contracts.”

4 ATTACK SURFACE SCANNING

Attack Surface scanning uncovers online cyber reconnaissance data that's normally hidden from your organisation. Gaining oversight of this data allows you to remediate the risks that would otherwise go unnoticed and unmitigated.

Assessment Checklist

□ Discover what web assets, domains and associated technologies are exposed to the internet

□ Assess risks for each component

□ Review severity of each risk

□ Plan remediation actions

> *"Attack Surface scanning shows what your organisation looks like through the eyes of a hacker."*

5 SECURITY TRAINING

Your staff have the potential to be your most effective line of security, or your biggest risk. With 76% of UK businesses affected by phishing attacks[3], it is therefore vital to ensure that all staff are aware of their security responsibilities and the consequences of their actions. Building these best practices into your day-to-day staff operations can dramatically reduce your risk of breaches.

Assessment Checklist

□ Conduct annual cyber security training for all staff members

□ Conduct social engineering/phishing campaigns to test training is effective

□ Build training into staff on-boarding process

□ Evaluate remote and on-site delivery options

□ Use technology to make training available 24/7 and accessible on multiple devices

□ Ensure training delivery can scale with business requirements

□ Monitor engagement and completion to ensure learning is embedded throughout the business

> *"Security training has the potential to be one of the most powerful tools in your cyber defence arsenal."*

[3] https://www.comtact.co.uk/blog/phishing-statistics-2019-the-shocking-truth

6 DEVICE SECURITY

Sensitive data is everywhere within an organisation, so security must span the full infrastructure stack, from servers to end-user devices. This includes both employee-owned and corporate-owned devices. These are all valid targets for hackers, so it is imperative that all devices within an organisation are kept secure against attack, regardless of who owns and manages them.

Assessment Checklist

- □ Enable 2FA wherever possible
- □ Mandate strong, unique passwords
- □ Deploy end-point anti-malware for all devices
- □ Use a VPN for connecting to corporate environment

"Creating and enforcing a strong BYOD policy can really boost your organisation's security."

7 GDPR

GDPR compliance isn't optional – it's a legal requirement as part of the Data Protection Act 2018. This means your organisation has to manage and maintain policies, processes and technical controls. Successfully maintaining GDPR can provide a real boost to customer confidence and greater data security.

Assessment Checklist

- □ Nominate a staff member to be accountable for data protection
- □ Undertake a gap analysis, including review of all policies and procedures
- □ Complete data flow maps and assess existing technical controls
- □ Create a step-by-step implementation plan
- □ Assign resources away from core business for implementation
- □ Resource on-going review and maintenance of GDPR compliance

"GDPR enables strong data protection controls that lower the risk of data breaches and costly fines."

8 MANAGED SIEM

A good SIEM solution can provide the greatest level of cyber protection when implemented correctly, but high staffing costs typically put true SIEM services out of reach of many organisations who need it. The inherent complexity and management overhead of SIEM technologies also make them expensive to run in-house and difficult to find value.

Assessment Checklist

- □ Source and configure a flexible SIEM platform
- □ Purchase and integrate threat intelligence feeds
- □ Deploy in all corporate environments, including on-premises, cloud, container & serverless
- □ Hire security analysts to run the SIEM, including investigating detected security events
- □ Create runbooks for each type of event
- □ Define clear reporting and escalation procedures

“Outsourcing to a managed SIEM provider gives 24/7 protection without the sky-high cost.”

9 CLOUD SECURITY

Cloud services sit at the core of modern businesses, most notably Microsoft Office 365. It operates on a shared responsibility model which leaves grey areas and misunderstandings that can lead to open doors for hackers. Regular security overviews are needed to give assurance that your cloud environment is configured correctly to keep your sensitive data secure.

Assessment Checklist

- □ Follow best practices for hardening
- □ Review every individual configuration option for security impact
- □ Assess shared responsibility on a per-supplier basis
- □ Evaluate and deploy additional controls, such as a VPN

“Don’t let productivity compromise your organisation’s security.”

10 PRIORITISE THREATS

Cyber threats come from a variety of places, with each representing a different risk to a business. Prioritising threats according to their severity allows organisations to gain maximum security for the lowest cost.

Assessment Checklist

- □ Collate all security threats from separate resources
- □ Rank threats by severity, using CVSS scoring
- □ Monitor active threats
- □ Track progress of remediation activities
- □ Highlight high-priority actions
- □ Create processes to support effective management

"Effectively managing threat priorities lets you allocate resources effectively to maximise security."

BULLETPROOF

STRONG SECURITY DOESN'T HAVE TO BE COMPLICATED

Schedule a free consultation with a Bulletproof security expert to see how you could simplify and strengthen your security posture.

BOOK YOUR FREE CONSULTATION TODAY

☎ 01438 532 900

www.bulletproof.co.uk

✉ contact@bulletproof.co.uk

ABOUT BULLETPROOF

Bulletproof is a trusted provider of innovative cyber security products and people-centric services. We help simplify and resolve the cyber security challenges for organisations across all industry sectors to protect their brand, value and assets against today's evolving threat landscape. Organisations of all sizes rely on our managed security solutions to protect and respond to cyber threats. Our dynamic portfolio of services includes CREST-certified penetration testing, threat monitoring services from our 24/7 SOC, VA scans, compliance consultancy, security training, GDPR & data protection and more. Find out more at www.bulletproof.co.uk