Our Assume Breach services

With our "Assume Breach" approach, our team of ethical hackers verify whether protection, detection and response mechanisms are implemented properly. We'll work with you to fix any weak spots discovered during the tests. In other words, we'll pinpoint issues before the cyber criminals do and ruin your business.

Identifying weak spots in your network infrastructure

Identifying vulnerabilities in your network infrastructure, no matter whether it is a network component or application, is critical when it comes to keep your sensitive data secure and your reputation intact. If these weak spots go unnoticed, you run the risk of compromise and unauthorised users accessing your data.

We've developed a standardised methodology for carrying out Assume Breach engagements. It consists of five standard attack scenarios, which can be complemented with more specific attacks depending on your requirements. These attack simulations are carefully coordinated with your teams to get the most out of the engagement and understand any weakness.

Our assessment attack scenarios are designed to help understand your security posture, your response to an attack and thus your maturity level. Altogether, our assessment is based on four phases to create a clear view.

So what is required?

It's about ensuring proactive protection of your brand, reputation and valuable electronic assets around the clock worldwide.

Secondly, it's about having a clear view of your overall risk profile from any potential financial impact, or as loss of customer trust which is very hard to recover.

At an operational level, it's also about understanding the countermeasures and actions that you may need to take if your information or services were compromised, as well as about having full visibility of your own security estate, your service providers and the services they are managing.

All of these combine to better support your organisation's business strategy.

Our Approach

1.We gather information

We'll start the reconnaissance phase of the assessment after we've collected and organised all the intelligence. Once the attack scenario has been established and initial access provided, we'll have a look around at the environment we find ourselves in. We'll interrogate the network and any other resources we may have access to when the projects kicks-off.

Any special user access level provided will be investigated such as file permissions, shares, ability to run software and other domain privileges. This knowledge will allow us to develop a plan of attack unique to each test. This phase may include processing passwords/password hashes, tokens and other methods of authentication. Using the processed system as a staging ground, we'll perform reconnaissance on the network associated with the device. This might include anything from sniffing to spoofing attacks to obtain additional network and domain information for further attacks.

2.We test for privilege escalation

During this phase of the assessment, we'll attempt to escalate privileges using the data obtained from the initial examination of the system during our reconnaissance phase. We may have discovered a misconfiguration, a vulnerability, or some sensitive information that could lead to greater permission levels. The goal of this phase is to access critical domain or system information to increase the permission level of the attacker on the system and throughout the target's network. This process may include running code as a user, rebooting a system or device and altering local configurations during the attack process.

3.We verify lateral movement possibilities

We'll attempt to laterally move through the network with credentials or other mechanisms of trust established during previous phases. We'll attempt to access other systems and network devices to expand the attack's sphere of influence.

4. We report our results to you

We'll then create a formal deliverable which describes the identified vulnerabilities and recommendations. If needed we're also able to create a presentation and discuss the results with a wider audience – it's up to you.

Our Attack Scenarios

- Inside attack - we'll act as a malicious employee working from within your office. This could be at any user or rights level.
- Successful deployment of malware - simulates an end user being the victim of malware. The malware can be "delivered" during a physical penetration, phishing attack or just by opening a "trojaned" file from a memory stick.
- Compromised service - a service has been exploited on a system providing an attacker a foothold. A common example would be a compromised web or network service located on the network.
- Compromised account - a user's account (username and password) has been exposed leading to other potential attack avenues. It may also include impersonation attacks.
- Rogue device - someone has compromised your office and connected a rogue device to your network. This can be a wireless access point or a device which creates a secure connection back to the attacker to provide access to the internal network.

Depending on your requirements we can also develop tailor-made attacks for you.

Never underestimate cyber criminals: "You don't know the power of the dark side."

Once a target is locked on by those who embrace the dark side, they don't let go and exhibit a persistence and creativity that is incredibly difficult to defend against. Cyber criminals are running a business just like you and they too need to deliver to be successful.

Why us?

We're experienced

In fact, we're one of the biggest security and business continuity practices in the world. We've got 3,600 security professionals working for us across the globe. And when it comes to ethical hacking, our team has more than 30 years' experience.

We operate across many industries, including industries that are significantly more advanced in dealing with cyber threats. This means we are ideally placed to bring expertise and know-how acquired with customers on the leading-edge of cyber security.

We're recommended

We're recognised as a Leader in ISG Provider Lens™ – Cyber Security – Solutions and Services 2024 in the UK. The report highlighted our strengths in managed security services, strategic security services, and technical security services in the UK.

BT has been named a Leader for the 20th consecutive year* in the 2024 in the Gartner Magic Quadrant™ for Global WAN Services based on its "Ability to Execute and Completeness of Vision".

*Magic Quadrant for Global WAN Services was previously named Magic Quadrant for Network Services, Global

We're qualified and security cleared

Our consultants hold industry certifications like CISSP, CISA, OSCE, and OSCP.

Where appropriate, our consultants possess national security clearance for delivery to government customers.

We're accredited for ISO27001:2013 covering our security testing services to both internal and external customers. Next to our ISO27001 accreditation we're also accredited for global consulting by Lloyd's Register Quality Assurance for the ISO9001 quality management system. We've held that since 2003 – proof of our long-term commitment to improving our services.

We have first-hand experience

As a large organisation, operating in around 180 countries, we know all about keeping our intellectual property, customers, people and premises safe.

We work hard to protect our networks, systems and applications – our ethical hackers and red team specialists test everything. Additionally, we work closely together with our blue team to test the effectiveness of our defences by carrying out multi-layered simulated attacks against both our physical and cyber security infrastructure.

This unrivalled experience, gained over many years of full spectrum testing of our policies, processes and defences, keeps our brand safe.

Find out more about ethical hacking

Learn more

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

JN: 1611673531 | November 2024.