TURNKEY

Prioritising business continuity with expert SAP penetration testing

Business profile

Turnkey's client is a global healthcare and pharmaceuticals group, delivering high quality products and medicines to people all over the world to prevent and treat diseases and keep them healthy.

The group's broad portfolio of medicines and R&D helps in a vast range of transformational areas including respiratory, consumer healthcare, oncology, HIV and vaccines against infectious diseases.

Highlights

- Report details risk level of all SAP vulnerabilities
- Prioritisations of what needs to be addressed
- Recommendations to mitigate future cyber threats
- Helping keep SAP landscape safe and secure

Challenge

SAP business systems are integral to Turnkey's client, controlling the group's financial and compliance reporting responsibilities and Segregation of Duties (SoD) as well as its consumer products and vaccine health systems.

With over 20 SAP systems requiring testing, the Turnkey service is helping this global pharmaceutical business to keep their SAP systems safe.

As part of their controls and compliance framework, the pharmaceuticals group need to carry out SAP exploitable vulnerability assessments every year. Turnkey Consulting had been engaged in 2019 to carry out vulnerability scanning and provide assurances, together with recommendations and reporting on the health of the group's SAP systems.

But the pandemic over the past year had brought different challenges to the business with many of their production systems having an extended period of downtime, coupled with the pharmaceutical industry pressures of the global vaccination programme. As a result, the time required for fixing and patching vulnerabilities had been reduced and there was a debate over the requirements, extent and cost of repeating a vulnerability scanning programme, which was likely to render similar results as the previous year.

Benefits

Explore all vulnerabilities: The report exposes weaknesses in the group's SAP systems, applications, network, infrastructure and other gateways that are linked to SAP, so that they can be prioritised in order of business-critical factors.

Business continuity: The group's business operations are kept seamlessly up-and-running 24/7 and any potential disruptions and negative impacts are quickly identified. Penetration testing uncovers potential threats and ensures that the group does not incur downtime or a loss of productivity.

Simulated attacks provide oversight of real-life risks: Penetration testing provides Turnkey's client with oversight of the impact of real-life criminal methods and activities and how these might be mitigated.

Prioritise which vulnerabilities to address first: The group can prioritise which exploitable vulnerabilities need addressing in order of importance to ensure minimal impact on the business.

Solution

Following a consultation with Turnkey, the group was advised that a blended penetration and red team test could be a more appropriate pathway and would meet the needs for annual SAP compliance checks. The penetration testing approach recognises that there will inevitably be inherent vulnerabilities but focuses on prioritisation and business risk, to help answer the bigger questions such as whether the group can rely on its SAP systems to run its business processes and the extent to which it is protected from data disclosure.

Penetration testing approach and methodology

Using the standard approach of deploying a pre-production system to reduce the minor risk of damage to any live systems, Turnkey set about working with key individuals within the group to gain a deeper understanding of the types of risk and concerns that the group had for their SAP estate.

The focus was on two main areas: the threat of cyber-attack and phishing. An attack could threaten the SAP systems that were connected to the internet, compromising the whole SAP estate, and phishing could result in unauthorised access and subsequent damage to any of the group's 20 SAP systems. For example, an SAP administrator who had their user name and password stolen, or following the theft of a company laptop.

Turnkey adopted MITRE ATT&CK, a standardised framework methodology that focuses on the chain of attack and uses penetration testing for simulated cyber threats, building realistic business scenarios that real-life criminals typically deploy to compromise an organisation's systems.

Taking the two scenarios that the group had highlighted, both risk of external attack and compromised credentials, Turnkey scoped and planted set-ups within the pre-production system using the MITRE ATT&CK framework, with the use of a company laptop, an SAP account and an IP address. While Turnkey performed these simulated attacks, only the group's security operations team were kept in the loop for legal protection reasons. Collaboration was key, and the group was kept up to date on a daily basis with initial findings.

The final output is a report that details the findings and risk level of all SAP vulnerabilities. It provides a prioritisation list and scopes out a vulnerabilities roadmap of how and what should be addressed, together with recommendations and future actions that will mitigate cyber threats.

With over 20 SAP systems requiring testing, the Turnkey service is helping this global pharmaceutical business to keep their SAP systems safe and secure against cyber criminals, improve overall SAP security and ensure business continuity.

Summary

"The report is a thorough and detailed output of where we recommend our client directs its efforts and budget in preventing attacks on its SAP systems and safeguarding ongoing trust in their business operations. This has been a successful and business-critical project for our pharmaceuticals client, who is very happy with the output".

TURNKEY

Turnkey Consulting
Contact: info@turnkeyconsulting.com
Visit: www.turnkeyconsulting.com

SAP Partner