Wie gut sind Sie auf Hackerangriffe vorbereitet?

Ist Ihr Unternehmen wirklich bereit, Hackerangriffen standzuhalten? Schützen Sie Ihr Unternehmen effektiv genug vor den raffiniertesten Bedrohungen? Finden Sie es jetzt heraus, indem Sie eine umfassende Attack Simulation von CYSPA durchführen lassen.

Die jüngsten Hackerangriffe auf Swisspro, Radio Top und Schneider Software haben eindrücklich aufgezeigt, wie raffiniert und professionell Cyberkriminelle vorgehen und wie viel Schaden so genannte **Ransomware** verursachen kann.

CYSPA bietet Ihnen die Möglichkeit, die Sicherheitsmassnahmen und Widerstandsfähigkeit Ihres Unternehmens mit einer massgeschneiderten **Attack Simulation** zu testen. Unsere Experten führen eine **realistische** und **kontrollierte Nachstellung** von **Hackerangriffen** durch, um Schwachstellen aufzudecken und potenzielle Risiken zu identifizieren. Dabei werden dieselben Tools und Methoden eingesetzt, wie bei realen Angriffen.

Durch enge Koordination mit den firmeninternen Ansprechpartnern wird sichergestellt, dass es dabei zu **keinen Schäden oder Unterbrechungen** kommt. Sämtliche Resultate werden in einem **Schlussbericht** zur Verfügung gestellt. In diesem erhalten Sie Informationen zur **Widerstandsfähigkeit** Ihres Unternehmens gegen Ransomware sowie eine detaillierte Auflistung aller **Risiken** mit **Massnahmenempfehlungen**.

CYSPA GmbH | www.cyspa.ch | +41 41 521 61 61 | info@cyspa.ch

CYSPA
CYBER SECURITY PARTNERS

Ablauf Attack Simulation

Kick-Off Meeting und Projektplanung

Beim Kick-Off Meeting werden die Ansprechpartner bzw. die Projektorganisation, Termine und der detaillierte Projektablauf definiert und festgehalten. Ein NDA wird vorgängig unterzeichnet.

Social Engineering

Durch ein Phishing Awareness Test wird die Verwundbarkeit gegenüber Social Engineering Attacken überprüft.

Penetration Test extern

Mit dem externen Penetration Test werden die externen Angriffsflächen und allfällige Verwundbarkeiten aufgedeckt. Dazu werden sämtliche extern erreichbare Systeme einem Schwachstellen Scan unterzogen.

Penetration Test intern

In diesem Modul wird die Frage geklärt, was passiert, sobald ein Angreifer ins Unternehmensnetzwerk gelangt. Dabei werden interne Systeme auf Schwachstellen und die Widerstandsfähigkeit überprüft. Das Ziel ist es, die Kontrolle über das interne Netzwerk zu erlangen (Domain Admin).

Schlussbericht und Präsentation

Die Resultate der einzelnen Module werden geprüft, ausgewertet und analysiert. Die Erkenntnisse werden im Schlussbericht detailliert festgehalten, beschrieben und auf ihre Kritikalität bewertet. Zusätzlich erhalten Sie eine Liste mit Massnhamenempfehlungen. Danach wird der Schlussbericht in einer Präsentation dem gewünschten Kundenkreis stufengerächt und verständlich vorgestellt.

CYSPA
CYBER SECURITY PARTNERS

Durch eine Attack Simulation können Sie

vorhandene Sicherheitslücken aufdecken.

Unsere Experten simulieren reale Angriffsszenarien, um Schwachstellen in Ihren Systemen und Prozessen aufzudecken. Dadurch erhalten Sie wertvolle Einblicke und können gezielte Massnahmen ergreifen, um Ihre Sicherheit zu verbessern.

Ihre Cyber Risiken minimieren.

Eine Attack Simulation ermöglicht es, Schwachstellen und Sicherheitslücken zu identifizieren und proaktiv Massnahmen zu ergreifen, bevor Angreifer sie ausnutzen können.

das Vertrauen Ihrer Kunden stärken.

Durch das regelmässige Überprüfen und Verbessern Ihre Sicherheitsmassnahmen stärken Sie das Vertrauen Ihrer Kunden und Geschäftspartner. Eine Attack Simulation zeigt, dass Sie die Sicherheit ernst nehmen und aktiv gegen Bedrohungen vorgehen.

Sind Sie bereit, die Widerstandsfähigkeit Ihres Unternehmens zu testen?

Verlassen Sie sich nicht nur auf Vermutungen, sondern lassen Sie Ihre Sicherheitsmassnahmen realistisch überprüfen. Mit einer **Attack Simulation** von CYSPA erhalten Sie wertvolle Erkenntnisse, um Ihre Widerstandsfähigkeit gezielt zu optimieren.

Kontaktieren Sie uns noch heute und erfahren Sie, ob Ihr Unternehmen wirklich gut genug vorbereitet ist, um Hackerangriffe abzuwehren und teure Betriebsausfälle zu vermeiden. Gemeinsam sorgen wir dafür, dass Ihre Daten und Ihre Reputation geschützt bleiben. Wir freuen uns auf Ihre Kontaktaufnahme.

Lieber heute in Informationssicherheit investieren, als morgen Lösegeld bezahlen!