NetUSE AG

25 Punkte Checkliste

zur Steigerung des IT-Security-Bewusstseins Ihrer Mitarbeitenden

Für mehr Informationen besuchen Sie bitte
www.NetUSE.de/awareness

Die Situation

In den letzten Jahren hat Deutschland eine Zunahme von Cyberangriffen verzeichnet, darunter Phishing-Angriffe, Ransomware-Attacken, Datendiebstahl und gezielte Angriffe auf Unternehmen und Behörden. Diese Angriffe können erhebliche wirtschaftliche, politische und soziale Auswirkungen haben.

Die Bedrohungslandschaft und die Techniken der Angreifer entwickeln sich ständig weiter. Cyberkriminelle nutzen fortschrittliche Methoden wie Social Engineering, Zero-Day-Exploits, Botnets und Advanced Persistent Threats (APTs), um in Netzwerke einzudringen und sensible Daten zu stehlen oder Schaden anzurichten.

Hinzu kommt die Entwicklung hin zur vermehrten Arbeit im Homeoffice, die nicht zuletzt durch die Coronakrise explosionsartig angestiegen ist sowie der Angriffskrieg auf die Ukraine, in dessen Rahmen deutlich vermehrt Cyberangriffe verzeichnet werden.

Die Welt der IT-Sicherheit ist komplex und ständig im Wandel. Es kann schwierig sein, mit den neuesten Bedrohungen, Angriffstechniken und Schutzmaßnahmen Schritt zu halten. Hinzu kommt, dass viele Mitarbeitende möglicherweise nicht das Fachwissen oder die Ressourcen haben, um sich mit den Details der IT-Sicherheit vertraut zu machen.

Wenn Mitarbeitende noch nie direkt von einem IT-Sicherheitsvorfall betroffen waren oder keine persönlichen Erfahrungen mit Phishing oder anderen Angriffen gemacht haben, können sie die Ernsthaftigkeit der Bedrohung möglicherweise nicht vollständig einschätzen bzw. nachvollziehen.

Oftmals wird das Bewusstsein für IT-Sicherheit erst dann geschärft, wenn man selbst oder jemand aus dem persönlichen Umfeld von einem Angriff betroffen ist.

In einer geschäftigen Arbeitsumgebung kann es ausserdem leicht passieren, dass Mitarbeitende IT-Sicherheitsrichtlinien ignorieren oder umgehen, um Zeit zu sparen oder bestimmte Aufgaben schneller zu erledigen. Beispielsweise könnten sie Passwörter wiederverwenden oder Dateien unverschlüsselt versenden, ohne die damit verbundenen Risiken zu berücksichtigen.

Wir von NetUSE wissen um dieses Sicherheitsrisiko und haben neben den klassischen Maßnahmen, um die Sicherheit der Unternehmens-IT zu festigen, auch den Faktor Mensch in unsere ganzheitliche Betrachtung mit einbezogen.

25 Punkte Checkliste

Wir geben Ihnen 25 Tipps an die Hand, die Sie dabei unterstützen, Ihre Mitarbeitenden für IT-Sicherheit zu sensibilisieren. Sie und Ihre Mitarbeitenden sind relevanter Teil Ihrer IT-Security Strategie!

1 Schulungen und Sensibilisierung

Führen Sie regelmäßige Schulungen und Sensibilisierungsmaßnahmen durch, um Ihre Mitarbeitenden über die verschiedenen Arten von Cyber-Bedrohungen und die besten Sicherheitspraktiken auf dem Laufenden zu halten.

2 Phishing-Simulationen

Führen Sie regelmäßige Phishing-Simulationen durch, um Ihre Mitarbeitenden mit Phishing-Angriffen vertraut zu machen und ihnen beizubringen, verdächtige E-Mails zu erkennen und darauf richtig zu reagieren.

3 Starke Passwortrichtlinien

Implementieren Sie starke Passwortrichtlinien, die die Verwendung von sicheren und eindeutigen Passwörtern erfordern. Stellen Sie sicher, dass Ihre Mitarbeitenden regelmäßig ihre Passwörter aktualisieren.

4 Zwei-Faktor-Authentifizierung

Ermutigen Sie Ihre Mitarbeitenden, die Zwei-Faktor-Authentifizierung zu verwenden, um ihre Konten und Systeme zusätzlich abzusichern.

5 Sicherheitsrichtlinien und -verfahren

Stellen Sie klare und verständliche Sicherheitsrichtlinien und -verfahren auf und stellen Sie sicher, dass alle Mitarbeitenden diese kennen und befolgen.

6 Regelmäßige Sicherheits-Updates

Stellen Sie sicher, dass alle Systeme, Anwendungen und Geräte regelmäßig mit den neuesten Sicherheitsupdates und Patches aktualisiert werden.

7 Datenschutz und vertrauliche Informationen

Sensibilisieren Sie Ihre Mitarbeitenden für den Schutz von vertraulichen Informationen und personenbezogener Daten. Erklären Sie, wie mit diesen umgegangen werden sollte und wie sie sicher aufbewahrt werden.

8 Sicherheitsbewusstsein im Umgang mit mobilen Geräten

Bringen Sie Ihren Mitarbeitenden bei, wie sie ihre mobilen Geräte sichern können und welche Risiken mit der Verwendung von öffentlichen WLAN-Netzwerken verbunden sind.

9 Verhaltensregeln für den Umgang mit E-Mails

Geben Sie klare Anweisungen zum Umgang mit E-Mails, insbesondere zur Erkennung von verdächtigen Anhängen, Links oder unerwünschten E-Mails.

10 Belohnungssysteme

Implementieren Sie Anreize und Belohnungen für Mitarbeitende, die gute Sicherheitspraktiken befolgen und Sicherheitsbedrohungen melden.

11 Sicheres Arbeiten im Homeoffice

Schulen Sie Ihre Mitarbeitenden in den besten Sicherheitspraktiken für das Arbeiten von zu Hause aus, einschließlich der sicheren Nutzung von VPNs und der Absicherung des Heimnetzwerks.

12 Social Engineering-Schulungen

Sensibilisieren Sie Ihre Mitarbeitenden für Social Engineering-Angriffe wie Phishing, Vishing (telefonisches Phishing) und Smishing (SMS-Phishing), damit sie betrügerische Versuche erkennen und darauf angemessen reagieren können.

13 Sicherer Umgang mit USB-Geräten

Weisen Sie Ihre Mitarbeitenden darauf hin, dass sie keine unbekannten oder verdächtigen USB-Geräte an ihre Computer anschließen sollten, da diese Malware oder andere Sicherheitsrisiken enthalten könnten.

14 Incident Reporting

Richten Sie einen klaren und einfachen Prozess für die Meldung von Sicherheitsvorfällen ein, damit die Mitarbeitenden verdächtige Aktivitäten oder potenzielle Sicherheitsverletzungen schnell melden können

15 IT-Sicherheitsbeauftragter

Bennen Sie eine:n Sicherheitsbeauftragte:n oder ein IT-Sicherheitsteam, das für die Umsetzung und Überwachung der Sicherheitsmaßnahmen verantwortlich ist und den Mitarbeitenden als Ansprechpartner:in für Sicherheitsfragen zur Verfügung steht.

16 Sicherheitsbewusstsein bei Software-Downloads

Sensibilisieren Sie Ihre Mitarbeitenden für die Risiken beim Herunterladen und Installieren von Software aus unsicheren oder unbekannten Quellen und ermutigen Sie sie, nur vertrauenswürdige Quellen zu verwenden.

17 Sicherheitsbewusstsein bei externen Dienstleistern

Geben Sie Anweisungen zum sicheren Umgang mit externen Dienstleistern und Drittanbietern, die Zugriff auf Systeme oder Informationen haben, um sicherzustellen, dass auch hier angemessene Sicherheitsvorkehrungen getroffen werden.

18 Kontinuierliches Feedback und Schulungen

Implementieren Sie ein Feedbacksystem, um Ihre Mitarbeitenden regelmäßig über ihre Sicherheitsleistung zu informieren und bieten Sie kontinuierliche Schulungen an, um ihr Wissen und ihre Fähigkeiten auf dem neuesten Stand zu halten.

19 Aktive Bedrohungsmitteilungen

Informieren Sie Ihre Mitarbeitenden aktiv über aktuelle Bedrohungen, Sicherheitswarnungen und neue Angriffsmethoden, um ihre Aufmerksamkeit auf relevante Sicherheitsrisiken zu lenken.

20 Regelmäßige Überprüfung und Aktualisierung von Sicherheitsrichtlinien

Überprüfen und aktualisieren Sie regelmäßig Ihre Sicherheitsrichtlinien und -verfahren, um sicherzustellen, dass sie den aktuellen Bedrohungen und Technologietrends entsprechen.

21 Regelmäßige Sicherheitsübungen

Führen Sie regelmäßige Sicherheitsübungen und Tests durch, um die Reaktion der Mitarbeitenden auf Sicherheitsvorfälle zu überprüfen und mögliche Schwachstellen in den Sicherheitsmaßnahmen aufzudecken.

22 Sicherheitsbewusstsein für Reisen

Schulen Sie Mitarbeitende, die berufsbedingt reisen, in den Sicherheitsrisiken und besten Praktiken während der Reise, einschließlich des Schutzes von Geräten und der Verwendung von sicheren Netzwerken.

23 Externe Experten und Schulungen

Holen Sie sich Unterstützung von externen IT-Sicherheitsexperten, um Schulungen, Audits und Sicherheitsbewertungen durchzuführen und sicherzustellen, dass Ihre Sicherheitsmaßnahmen den besten Branchenstandards entsprechen.

24 Sicherheitsbewusstsein bei BYOD

Wenn BYOD (Bring Your Own Device) erlaubt ist, informieren Sie die Mitarbeitenden über die Sicherheitsanforderungen und -richtlinien für ihre persönlichen Geräte und stellen Sie sicher, dass sie diese einhalten.

25 Sicherheitsbewusstsein als Teil der Unternehmenskultur

Stellen Sie sicher, dass IT-Sicherheitsbewusstsein als integraler Bestandteil der Unternehmenskultur wahrgenommen wird. Es sollte von der Unternehmensführung gefördert und von allen Mitarbeitenden unterstützt werden.

Diese 25 Punkte stellen einen Auszug der möglichen Maßnahmen dar, die ergriffen werden können, um das IT-Sicherheitsbewusstsein der Mitarbeitenden zu stärken.

Unser Tipp: Lassen Sie uns gemeinsam im Rahmen eines Assessments die konkrete Situation in Ihrer IT aufnehmen und daraus die wirklich notwendigen Maßnahmen ableiten.

Sensibilisierung für Phishing-Angriffe

In den letzten Jahren ist die Awareness, das Bewusstsein, für IT-Sicherheit und insbesondere für Phishing-Angriffe bei vielen Unternehmen und Mitarbeitern gestiegen. Die Medien haben vermehrt über Phishing-Angriffe und deren Auswirkungen auf Unternehmen berichtet, wodurch die Wichtigkeit von IT-Sicherheit verstärkt ins Bewusstsein gerückt ist.

Viele Organisationen haben reagiert und ihre Mitarbeitenden über Phishing-Angriffe und andere Formen von Social Engineering geschult. Schulungen und Sensibilisierungsprogramme werden häufig eingesetzt, um die Mitarbeitenden über die Risiken aufzuklären und ihnen beizubringen, wie sie verdächtige E-Mails identifizieren und darauf reagieren können.

Dennoch bleibt das Phishing eine der häufigsten und effektivsten Methoden, um Zugriff auf Systeme und Informationen zu erlangen. Cyberkriminelle passen ihre Taktiken ständig an, um Phishing-E-Mails glaubwürdiger und schwerer erkennbar zu gestalten. Es ist daher nicht ungewöhnlich, dass selbst gut geschulte Mitarbeitende gelegentlich auf Phishing-E-Mails hereinfallen.

NetUSE Phishing Kampagne

Tipp:

Mit unserem **Managed Service „NetUSE Phishing Kampagne“**, also eine in Punkt 2 empfohlene **Phishing Simulation**, helfen wir Ihnen dabei, Ihre Mitarbeitenden sukzessive für die Gefahren von Phishing-Mails zu sensibiliseren.

Mehr unter **www.NetUSE.de/awareness**

Die deutsche Regierung und verschiedene Organisationen setzen sich aktiv für die Stärkung der Cybersecurity ein. Es wurden Initiativen zur Verbesserung der IT-Sicherheit und zum Schutz kritischer Infrastrukturen gestartet. Zudem gibt es rechtliche Rahmenbedingungen wie das IT-Sicherheitsgesetz, um die Sicherheit in Deutschland zu stärken und Unternehmen zur Einhaltung bestimmter Standards zu verpflichten.

Seien Sie einen Schritt voraus und ergreifen Sie Maßnahmen, die die Sicherheit Ihrer IT deutlich erhöhen. Dabei können wir Sie unterstützen. Ob es dabei um die Umsetzung technischer Lösungen oder die Steigerung des IT-Sicherheitsbewusstseins Ihrer Mitarbeitenden geht, sind wir Ihr Partner.

Diese Checkliste wurde herausgegeben von der NetUSE AG.

NetUSE AG
Dr.-Hell-Straße 6
24107 Kiel

0431 2390-400
info@NetUSE.de
www.NetUSE.de