Penetrationstests
Leitfaden

Cluster Informationstechnologie
it-mitteldeutschland.de

Inhalt

Management Summary

Penetrationstests sind eine gängige Variante zur Aufdeckung vorhandener Schwachstellen in IT-Infrastrukturen. Die Gründe für das Auftreten von Schwachstellen können vielfältig sein. Veraltete Hard- & Software, Designfehler in verwendeten Produkten, Konfigurationsfehler aber auch unachtsame Mitarbeiter stellen hierbei nur Auszüge der Risiken dar, die Ihre Informationssicherheit gefährden können und die durch einen Penetrationstest sichtbar gemacht werden.

Damit ein Penetrationstest geeignete Ergebnisse liefern kann, kommen je nach Anwendungsfall unterschiedliche Standards, Vorgehensweisen, Werkzeuge aber auch durchführende Dienstleister in Betracht.

Die gängigsten Arten von Penetrationstests sind:

- Netzwerk-Pentest zur Überprüfung der Infrastruktur
- Anwendungspentest zur Überprüfung eigenentwickelter Software oder Web-Applikationen
- Social Engineering Pentest zur Überprüfung, ob Mitarbeiter anfällig für den Diebstahl von Zugangsdaten, die Preisgabe sensibler Informationen oder das Ausführen von schadhaften Dateianhängen sind
- Physischer Pentest zur Überprüfung der Absicherung von Gebäuden und sensiblen Bereichen
- Red Team Pentest, zur Überprüfung der getroffenen Schutzmaßnahmen unter weitgehend realistischen Angriffsbedingungen.

Die Auswahl eines geeigneten Dienstleisters sollte maßgeblich auf Grundlage des zu prüfenden Umfangs getroffen werden, da die Anbieter häufig sehr spezialisiert auf eine bestimmte Pentest-Art sind. Weitere wichtige Kriterien sollten unter anderem die Seriosität, die offene Kommunikation über Testmethodik, eigene Fähigkeiten und Risiken sowie eine vertragliche Zusicherung zur Vertraulichkeit vor-, während- und nach dem Pentest sein. Besondere Vorsicht ist bei „schwarzen Schafen“ der Branche geboten, die unaufgefordert und ohne vorherige Genehmigung Systeme prüfen und anschließend versuchen die Legitimation und Bezahlung über eine nachträgliche Beauftragung zu erzielen.

Der Abschlussbericht eines Penetrationstests kann je nach Art und beauftragtem Umfang sehr komplex und lang ausfallen. Folgende Inhalte, die den Anforderungen an Transparenz und Nachvollziehbarkeit gerecht werden, sowie grundlegende Aussagen zum Kontext sollten enthalten sein und hier beispielhaft Erwähnung finden:

- Management-Summary; vertragliche Rahmenbedingungen über Art, Umfang, Zielstellung und Testmethodik des Pentests; Rechtliche Rahmenbedingungen zu Risiken, Vertraulichkeit, Haftung und Datenschutz; verwendete Werkzeuge und technische Details; gefundene und ausgenutzte Schwachstellen; Testergebnisse und Maßnahmen zur Behebung.

Der Abschlussbericht sollte tunlichst als Grundlage für Verbesserungsmaßnahmen dienen. Diese können sowohl organisatorischer oder technischer Art sein, je nachdem, was im Test festgestellt wurde. Die Überarbeitung von Unternehmensprozessen, die Umkonfiguration oder Härtung von Systemen, die Anschaffung neuer und moderner Systeme oder auch die Sensibilisierung der Mitarbeiter durch Awarenesstrainings stellen hierbei nur einen Auszug dar. Sollte Ihnen die Umsetzung geeigneter

Maßnahmen zu komplex erscheinen, gehen Sie gerne auf geeignete Dienstleister zu, die Sie dabei unterstützen können.

Warum Pentests sinnvoll sind?

Die voranschreitende Digitalisierung erfordert die laufende Beachtung der Informationssicherheit in Unternehmen und öffentlichen Einrichtungen durch die Geschäftsführung. Nachholbedarfe zeigen sich hierbei insbesondere in Mittelstandsunternehmen, bei denen das Risikobewusstsein und die getroffenen Vorsorgemaßnahmen noch nicht so ausgeprägt sind wie in Großunternehmen oder Konzernen. Die Einführung vernetzter Geräte, neuer Softwareprodukte oder Internetdienste bietet neben den Vorteilen für die Geschäftsgestaltung auch Risiken, die stets mit bedacht werden sollten. So können über unsicher konfigurierte Schnittstellen oder Programmierfehler in den Softwareprodukten, sogenannten Sicherheitslücken, unerwünschte Angriffsflächen für die Institution entstehen, die durch Cyberkriminelle ausgenutzt werden können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt im Bericht zur Lage der IT-Sicherheit in Deutschland 2022 an, dass 2021 insgesamt 20.174 Sicherheitslücken in Programmen entdeckt werden konnten, was einem Anstieg zum Vorjahr von ca. 10 Prozent entspräche. 56 Prozent der auftretenden Sicherheitslücken wurden mit einer hohen oder kritischen Bewertung versehen.[1]

Um diesen Risiken angemessen zu begegnen, bieten sich neben dem regelmäßigen Einspielen von Sicherheitsupdates insbesondere Penetrationstests an. Hierbei werden ausnutzbare Sicherheitslücken in der Systemumgebung identifiziert, damit diese anschließend durch geeignete Maßnahmen geschlossen werden können.

Neben den zuvor angeführten Gründen gibt es auch gesetzliche Anforderungen, die ein Unternehmen dazu verpflichten, regelmäßig Sicherheitsüberprüfungen durchzuführen. Beispielhaft hierfür können die Sicherheitsanforderungen an digitale Gesundheitsanwendungen (DiGA) des Bundesinstituts für Arzneimittel und Medizinprodukte, die Anforderungen an intelligente Messsysteme (Smart Meter Gateways) gem. TR-03109 des BSI, Sicherheitsvorgaben für den Zahlungsverkehr bei Kreditkartenzahlungen gem. PCI-DSS oder auch Anforderungen an die Produktsicherheit „smarter Produkte“ gemäß Entwurf des EU Cyber Resilience Act dienen. Darüber hinaus sind regelmäßige Validierungen und Anpassungen getroffener Sicherheitsmaßnahmen ein Erfordernis der EU-DSGVO, von Zertifizierungen (z.B. DIN ISO 27001, BSI-Grundschutz), von Sicherheitsaudits oder auch Wirtschaftsprüfungen.

Doch auch ohne diese Verpflichtungen lohnt es sich, in die IT-Sicherheit zu investieren, da die Kosten für einen erfolgreichen Hackerangriff oft deutlich höher ausfallen können als die Kosten für präventive Maßnahmen. Außerdem kann ein Pentest helfen, das Vertrauen der Kunden in die Sicherheit des Unternehmens zu stärken.

[1]Vgl. Bundesamt für Sicherheit in der Informationstechnik (10/2022), Die Lage der IT-Sicherheit in Deutschland 2022, S. 33, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410

Welche Arten von Pentests gibt es?

Penetrationstests seriöser Anbieter folgen internationalen Standards, die ein Maß an Güte und zu verwendende Testszenarien vorsehen. Die Tests sind im Kern vergleichbar, weisen aber Unterschiede in den gesetzten Rahmenbedingungen oder auch dem Einsatzfeld auf. Folgend sollen gängige Anwendungsfelder für Penetrationstests näher betrachtet werden.

Netzwerk-Pentest

Ein Netzwerk-Pentest konzentriert sich auf die Netzwerksicherheit und prüft, ob Angreifer in der Lage sind, von außen auf das Netzwerk zuzugreifen und/oder darin mit anderen IT-System zu interagieren. Dabei werden Schwachstellen in der Netzwerkinfrastruktur, wie zum Beispiel ungesicherte Netzwerkgeräte oder unzureichend bzw. fehlerhaft konfigurierte Perimeter-Sicherheitsmaßnahmen (z.B. Firewalls), ausgenutzt.

Fallbeispiel

Der Penetrationstest der Systemumgebung fördert zutage, dass auf einem der VPN-Gateways keine Multi-Faktor Authentifizierung konfiguriert wurde. Die über eine Phishingmail von den Mitarbeitern erhaltenen Zugangsdaten erlauben dem Penetrationstester den initialen Zugriff auf die Unternehmensumgebung. Durch den Penetrationstest erhält die IT-Administration Kenntnis über die Schwachstelle und kann das VPN-Gateway sicher konfigurieren. Anschließend ist ein Fernzugriff nur noch durch die Kombination von Zugangsdaten und einem Einmalpasswort möglich.

Anwendungspentest

Ein Anwendungspentest bezieht sich auf eine bestimmte Anwendung, meist eine Webanwendung (Web-Application). Dabei werden Sicherheitslücken in der Anwendung oder Schwachstellen in der Authentifizierung aufgedeckt.

Fallbeispiel

Der Penetrationstest der Webseite / des Webshops fördert zutage, dass ein veralteter Apache-Webserver verwendet wird. Die bereits bekannten Sicherheitslücken für die verwendete Version könnten es einem Angreifer ermöglichen einen Denial-of-Service (Nicht-Erreichbarkeit der Webseite) zu verursachen, wodurch die Geschäftstätigkeit beeinträchtigt wird. Aufgrund des Penetrationstests kann hier nachgesteuert und die Systeme aktualisiert werden, wodurch das Risiko eines Ausfalls der Website / des Webshops reduziert werden kann.

Social Engineering Pentest

Social Engineering Pentests konzentrieren sich auf die menschliche Seite der Sicherheit und prüfen, wie anfällig Mitarbeiter für soziale Manipulationstaktiken sind. Hierbei werden Taktiken wie Phishing, Spear-Phishing, Vishing, Pretexting und Baiting verwendet, um Mitarbeiter zu täuschen und vertrauliche Informationen zu erlangen.

Fallbeispiel

Im Pentest wird es gestattet Phishing Mails an die Mitarbeiter zu versenden, um die Sensibilität der Mitarbeiter für diesen Angriffsvektor nach vorhergehenden Schulungsmaßnahmen zu überprüfen. Trotz der Schulung klicken manche Mitarbeiter auf kompromittierte Dateianhänge oder geben Ihre Zugangsdaten in gefälschte Eingabemasken ein. Dies wird durch den Pentest sichtbar, woraufhin andere Schulungsszenarien oder weitere technische Schutzmaßnahmen ergriffen werden können.

Physischer Pentest

Bei einem physischen Pentest wird untersucht, wie leicht Angreifer physischen Zugang zu einem Gebäude oder einer Einrichtung erlangen können. Dabei werden Schwachstellen wie ungesicherte Türen oder unzureichende Überwachungssysteme ausgenutzt.

Fallbeispiel

Der Serverraum befindet sich im Erdgeschoss des Gebäudes und verfügt über ein nicht vergittertes oder alarmgesichertes Fenster. Ein Zutritt ist mit einfachen Maßnahmen möglich, da es sich um ein Standardfenster handelt. Ein echter Angreifer hätte volle Zugriffe auf die Systeme, Speichermedien nehmen oder diese in Ruhe entwenden können.

Red Team-Pentest

Bei einem Red Team-Pentest wird eine Gruppe von Sicherheitsexperten beauftragt das Unternehmen wie real agierende Eindringlinge anzugreifen. Hierbei werden alle verfügbaren Techniken und Tools eingesetzt, um Schwachstellen im System zu finden und auszunutzen. Das Ziel ist es die Abwehrmaßnahmen des Unternehmens zu testen und zu verbessern.

Fallbeispiel

Bei einem Red Team-Test greifen die engagierten Angreifer (Red-Team) die getroffenen Sicherheitsmaßnahmen mit realistischen und aktuellen Angriffsmethoden an. Ziel ist es Lücken im weiten Feld der verschiedenen Abwehrmechanismen zu finden. Die IT-Administratoren des Zielunternehmens können kooperierend an dieser Übung teilnehmen, um etwa die Detektions- und Reaktionsfähigkeiten zu testen. Die erkannten Lücken können anschließend geschlossen werden.

Wie sehen die wirtschaftlichen Aspekte aus?

Unternehmen investieren bereits viel Zeit und Ressourcen in die Absicherung Ihrer IT-Infrastruktur. Dennoch bestehen häufig, insbesondere in Mittelstandsunternehmen, Nachholbedarfe, da die verwendeten Systeme und Sicherheitsstrategien aufgrund vielfältiger Gründe nicht immer zeitnah mit der aktuellen Bedrohungsentwicklung mithalten können. Ein Penetrationstest kann bei der regelmäßigen Bewertung getroffener Sicherheitsmaßnahmen und der dafür aufgewandten Investitionen behilflich sein, indem die Wirksamkeit der getroffenen Maßnahmen und etwaige Optimierungspotentiale frühzeitig sichtbar gemacht werden. Darüber hinaus kann er gravierende Sicherheitsgefährdungen, beispielsweise technisch enorm veraltete

Systeme, sichtbar machen, die in zukünftigen Budgetplanungen und Risikoanalysen Berücksichtigung finden sollten, bevor es Angreifern gelingt diese Schwachstellen aktiv auszunutzen.

Kosten vs erwarteter Output

Die Kosten für einen Pentest variieren je nach Umfang, Komplexität und Dauer des Tests. Ein umfassender Pentest kann mehrere tausend Euro kosten und erfordert eine intensive Vorbereitung und Durchführung.

Berücksichtigt werden sollten jedoch auch die Kosten, die zur Bewältigung eines erfolgten Cyberangriffs aufgewandt werden müssen und die die Kosten für präventive Sicherheitsmaßnahmen in der Regel deutlich übersteigen. Die Nennung einer detaillierten Kostensumme ist unter realistischen Betrachtungen nicht möglich, da die Unternehmen, die Angriffsvarianten, die betroffenen Systeme, vorhandene Verfahren und Prozesse sowie weitere Variablen je Unternehmen und Cyberangriff sehr variieren können.

Um dennoch einen Ansatzpunkt zur individuellen Ermittlung etwaiger Kosten eines Cybersicherheitsvorfalls geben zu können, möchten wir gängige Kostenpositionen anführen, die bei der Bewältigung eines Cybersicherheitsvorfalls anfallen können:

- Geschäftsbeeinträchtigungen oder Betriebsstörungen durch Ausfall relevanter Systeme oder Produktionsanlagen, bis hin zum kompletten Betriebsstillstand
    - Die geschätzte Ausfallzeit im Zuge eines mittelschweren Cyberangriffs im Mittelstand kann mit ca. 21 Tagen angenommen werden
- Kosten zur Beseitigung der unmittelbaren Schäden und Reparaturen an betroffenen Systemen
    - Die geschätzten Kosten zur vollständigen Bereinigung und Neuinstallation eines Nutzercomputers können mit ca. 400€ pro Gerät angenommen werden
    - Die Wiederherstellungskosten für Serversysteme können deutlich höher ausfallen
- Kosten zur Beschaffung neuer Geräten oder Systemkomponenten nach einer Beschädigung
- Kosten für externes Personal zur Vorfallbewältigung
    - Z.B. IT-Forensik, Anwälte, Teams zur Krisenkommunikation, Sicherheitsspezialisten
- Zusätzliche Aufwände für die Beantwortung vermehrter Kundenanfragen
- Kosten durch etwaige Bußgelder im Zuge von Rechtsverletzungen oder Vertragsstrafen
- Kosten durch entwendete sensible Daten
- Steigende Versicherungspolicen oder Aufkündigung des Vertrages durch die Versicherung
- Kosten für eine etwaige Lösegeldzahlung bei einer Verschlüsselung durch Ransomware
- Reputationsverluste bei Kunden, Partnern, Aktionären usw.
- Enorme Arbeitsbelastungen für das eigene Personal durch Mehrarbeit bei der Vorfallbewältigung
    - Folgen können z.B. sein: Moralverlust, Depressionen, Schlafstörungen, Burnout, körperliche Beschwerden

Ein erfolgreicher Angriff auf die IT-Infrastruktur eines Unternehmens kann die gesamte Organisation gefährden. Die Durchführung regelmäßiger Penetrationstests kann gezielt Schwachstellen im Unternehmen identifizieren und bei der Beseitigung helfen, bevor es zu einem erfolgreichen Angriff kommt. Dadurch können Risiken für das Unternehmen und die verantwortlichen Geschäftsführer reduziert und letztlich viel Geld gespart werden.

Kostenreduktion durch bewusste Eingrenzung des Scopes

Durch eine Eingrenzung des Scopes, also des Testumfangs, auf bestimmte Systeme innerhalb der IT-Infrastruktur können die Kosten für einen Penetrationstest reduziert werden, da in der Regel der Testaufwand geringer ausfällt. Eine solche Eingrenzung kann jedoch auch dazu führen, dass bestimmte Schwachstellen unentdeckt bleiben und somit weiterhin unentdeckte Risiken für das Unternehmen bestehen können. Es ist wichtig, dass bei der Eingrenzung des Scopes sorgfältig vorgegangen wird und sichergestellt ist, dass die wichtigsten Bereiche der IT-Infrastruktur abgedeckt sind. Eine umfassende Risikoanalyse kann helfen die wichtigsten Bereiche zu identifizieren, die getestet werden sollten.

Fördermöglichkeiten

Um die Kosten für Pentests zu reduzieren, gibt es auch verschiedene Fördermöglichkeiten. Informationen über etwaige Fördermöglichkeiten können bei Branchenverbänden oder zuständigen öffentlichen Stellen eingeholt werden.

Zusammenfassend lässt sich sagen, dass Pentests ein wichtiger Schritt bei der Absicherung der IT-Infrastruktur in Unternehmen sind. Die Kosten für Pentests können je nach Umfang variieren und mehrere Tausend Euro umfassen. Eine bewusste Eingrenzung des Scopes kann die Kosten reduzieren, jedoch sollten die wichtigsten Bereiche der IT-Infrastruktur zwingend durch den Test abgedeckt werden. Weitere Kostenreduktionen lassen sich durch die mögliche Nutzung verfügbarer Fördermöglichkeiten erzielen.

Welche rechtlichen Grundlagen gibt es?

Penetrationstest berühren die innersten Belange eines Unternehmens. Die wichtigsten Daten, Verfahren und Schwachstellen innerhalb des Unternehmens werden durch die Testdurchführenden angegriffen bzw. aufgedeckt. Für Unternehmen ist es naturgemäß schwierig sich dem zu stellen, insbesondere wenn keine vorherigen Beziehungen zum Tester oder dessen Unternehmen bestehen. Daher sind das Verständnis, die Kommunikation und das Leben von ethischen Leitlinien der Testanbieter im professionellen Umfeld essenziell.

Zu den ethischen Grundsätzen von Penetrationstests gehören:

- Keine Tests ohne vorherige Genehmigung
- Ehrliche Kommunikation eigener Fähigkeiten und des Risikos der Tests
- Verschwiegenheit vor, während und nach dem Projekt
- Keine Vorteilnahme durch gewonnene Erkenntnisse, keine Mitnahme von Daten
- Integrität gegenüber Mitarbeitern des Auftraggebers, besonders beim Social-Engineering

Vorsicht ist insbesondere bei den schwarzen Schafen der Industrie geboten, die ungefragt und ohne Erlaubnis Systeme „prüfen“ und bei Erfolg die Betroffenen quasi erpressen, damit diese durch eine nachträgliche Beauftragung und Bezahlung den Penetrationstest rückwirkend legitimieren.

Ein Penetrationstest ist von einem echten Angriff zunächst nicht zu unterscheiden. Die Gesetze sind dennoch einzuhalten, so existiert in Deutschland etwa der sogenannte Hackerparagraf §202a ff. StGB, der das Ausspähen

und Abfangen von Daten, die Umgehung von Schutzmechanismen sowie die Nutzung von dazu geeigneten Werkzeugen unter Strafe stellt. Ebenso bestehen seitens des Auftraggebers Pflichten zum Schutz der eigenen und Kundendaten (EU-DSGVO), sowie gegenüber den eigenen Mitarbeitern bei der Verwendung von Social-Engineering Praktiken.

Penetrationstests sollten von beiden Parteien aus Eigeninteresse gut vorbereitet werden, damit geltende Gesetze und Vorgaben erfüllt werden können. Der Auftraggeber muss sich mit dem potenziellen Partner eine Vertrauensbasis erarbeiten, die in entsprechenden Verträgen und Genehmigungen ihren schriftlichen Ausdruck findet.

Mindestens folgende Aspekte sind vertraglich zu fixieren:

- Auftragnehmer und Auftraggeber inkl. möglicher Drittparteien
- Klärung der Eigentumsverhältnisse bzw. Verantwortlichkeiten (Systeme, Daten, Personen)
- Systeme und Umfang/ Tiefe der Testdurchführung (Scope) und der Testzeitraum
- Notfallkontakte und -maßnahmen

Falls der Auftraggeber zu testende Dienste und Systeme bei einem externen Dienstleister betreibt oder etwa Leistungen (z.B. Webhosting) angemietet hat, ist der externe Dienstleister vor Testbeginn in die Testplanung einzubeziehen, da dieser ggf. der Eigentümer der zu testenden Infrastruktur ist und seine Erlaubnis oder Verweigerung erteilen muss.

Zur Gewährleistung der Integrität bei der Informationsverarbeitung sollte der Auftragnehmer geeignete Methoden vorstellen, die die Vereinbarungen nachweisbar erfüllbar machen, so dass das Vertrauen nur noch dem Faktor Mensch entgegengebracht werden muss.

Welche Inhalte sollte ein Pentest-Bericht enthalten?

Nach Abschluss der aktiven Testphase erstellt der Penetrationstester in der Regel einen detaillierten Abschlussbericht. Ein detaillierter Bericht ist unerlässlich, um den Kunden umfassend über den Pentest zu informieren und den Ansprüchen an Nachvollziehbarkeit und Transparenz gerecht zu werden.
Neben einer Management Summary, die die wichtigsten Testergebnisse zusammenfasst, sollten auch ein Überblick über die beauftragten Leistungen, Leistungsinhalte, Testgrenzen (Scope), mögliche Risiken, rechtliche Aspekte und auch die Zielstellung und die Prüfkriterien enthalten sein.

Ein guter Pentest-Bericht sollte detaillierte Informationen über die gefundenen Schwachstellen enthalten und auch empfohlenen Maßnahmen zur Behebung dieser Schwachstellen anführen. Der Bericht sollte auch die Methoden und relevanten technischen Details beschreiben, die beim Pentest verwendet wurden und die dem Kunden helfen die Schwachstellen und Zusammenhänge zu verstehen und die für die Behebung wichtig sind.

Ein weiterer wichtiger Aspekt des Pentests ist die Dokumentation der Durchführung. Ein guter Pentester sollte eine sorgfältige Dokumentation über den gesamten Testprozess führen. Dies umfasst alle Schritte, die unternommen wurden, um Schwachstellen zu identifizieren, sowie alle Tools, die verwendet wurden. Es ist auch

wichtig, die Ergebnisse des Tests sorgfältig zu dokumentieren, einschließlich aller gefundenen Schwachstellen und der empfohlenen Maßnahmen zur Behebung dieser Schwachstellen.

Im Idealfall sollte der Pentest-Bericht auch eine Liste der Nachweise enthalten, die bei Bedarf an Geschäftspartner weitergegeben werden können. Diese Nachweise können dazu beitragen, das Vertrauen in die Sicherheitsmaßnahmen des Unternehmens zu stärken und Geschäftspartner davon zu überzeugen, dass angemessene Maßnahmen zur Absicherung des Unternehmens getroffen wurden. Zu diesen Nachweisen können beispielsweise Screenshots, Protokolle oder andere Beweise gehören, die die Durchführung des Pentests belegen.

Abschließend sollten Informationen zum Ethical Kodex bei der Testdurchführung, Neutralität des Durchführenden sowie datenschutzrelevante Informationen zu Aufbewahrung, Archivierung, Löschfristen usw. angeführt sein.

Was ist, wenn mein Unternehmen Schwachstellen aufweist?

Die Ergebnisse des Pentests sollten als Ausgangsbasis für Verbesserungsmaßnahmen dienen, um die Sicherheit des Unternehmens weiter zu verbessern. Aufgedeckte Schwachstellen gilt es zu schließen. Je nach Art und Scope des Pentests können hierbei unterschiedliche Prioritäten und Verfahrensweisen sinnvoll sein. Beispielhaft hierfür können die folgenden Vorgehensweisen sein, die jedoch keinen Anspruch auf Vollständigkeit erheben:

- Aufgedeckte bekannte Sicherheitslücken, die etwa auf veralteten Systemen auftreten können, lassen sich häufig durch bereits vorhandene Herstellerupdates schließen.
- Für neue Sicherheitslücken existieren häufig sogenannte „Workarounds“ der Hersteller, durch die mithilfe einer angepassten Systemkonfiguration das Risiko einer Verwundbarkeit reduziert und der Zeitraum bis zur Verfügbarkeit eines Herstellerupdates überbrückt werden kann.
- Fehlerhafte Konfigurationen können durch eine Anpassung der Systemeinstellungen behoben werden
- Fehler in einem Quellcode eigenentwickelter Software können häufig durch Ihre Entwickler behoben werden
- Sollten Phishing-Methoden beim Pentest erlaubt und erfolgreich gewesen sein, können Mitarbeiter häufiger sensibilisiert oder weitere technische Schutzmaßnahmen ergriffen werden

Generell betrachtet sollten die erkannten Schwachstellen in Abhängigkeit von der verfolgten Sicherheitsstrategie, den Risikomanagement- und Patchmanagement-Prozessen, der Kritikalität der entdeckten Schwachstellen und den eigenen Möglichkeiten behandelt werden.

Eine aktive Kommunikation mit den verwendeten IT-Dienstleistern und Lieferanten erachten wir als sinnvoll, da diese maßgeblich bei der Behebung der erkannten Sicherheitslücken unterstützen können. Ob hierbei auf bereits verwendete Dienstleister, zu denen ein Vertrauensverhältnis besteht und die die Systemumgebung bereits kennen oder auf neutrale externe Dienstleister gesetzt werden soll, unterliegt dabei der freien Wahl der Unternehmensführung. Die Behebung der Schwachstellen sollte im Anschluss überprüft und dokumentiert werden. Dies gilt insbesondere bei der Anwendung von „Workarounds“, da diese häufig zu einem späteren

Zeitpunkt rückgängig gemacht werden müssen, sobald ein reguläres Herstellerupdate verfügbar ist und eingespielt wurde.

Da jeder Penetrationstest unterschiedlich verläuft, sich die Unternehmensumgebung regelmäßig ändern kann und die Sicherheitsanforderungen und Sicherheitsbedrohungen zukünftig andere sein können, empfiehlt es sich einen Penetrationstest in regelmäßigen Abständen zu wiederholen. Da auch Pentester mit verschiedenen Werkzeugen arbeiten und unterschiedliche Fähigkeiten, Erfahrungen und Herangehensweisen besitzen, ist es immer eine gute Idee diese auch mal zu wechseln. Hierdurch bekommt der Auftraggeber neue Eindrücke und zusätzliche Perspektiven, die bei der Absicherung des Unternehmens sinnvoll unterstützen können.

Glossar

Verfasser

Dieses Whitepaper ist im Rahmen eines unternehmensübergreifenden Austausches unter dem Dach des Cluster Informationstechnologie Mitteldeutschland entstanden. Wir bedanken uns recht herzlich bei allen, die an der der Entstehung dieses Dokumentes und dessen gelingen mitgewirkt haben.

KUPPER
IT. innovativ. effizient. sicher.

Tarek Winter (IT-Sicherheitsberater & ISB)
tarek.winter@kupper-it.com

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

Dr. Sandro Wefel (Institut für Informatik)
sandro.wefel@informatik.uni-halle.de

MGID

Thomas Reiche (Geschäftsführer, CISSP & CHFI)
thomas.reiche@mgid.de

Felix Böge (IT-Sicherheitsberater)
felix.boege@mgid.de

PYUR
Business

Martin Leipziger (Senior Solution Architect)
martin.leipziger@pyur.com

Matthias Ernerth (Solution Architect)
matthias.ernerth@pyur.com

softline
Group

Ulf Seifert (Technical Lead IT- und IS & ISB)
ulf.seifert@softline-group.com

staffadvance

Torsten Kauerauf (Projektmanager, ISB & DSB)
torsten.kauerauf@staffadvance.com

Cluster
Informationstechnologie
it-mitteldeutschland.de