



Leitfaden zur Durchführung von Penetrationstests von IT-Systemen, -Applikationen und -Netzen in der Bundesverwaltung

vom 13. Februar 2002

1. Zweck des Dokumentes

Der vorliegende Leitfaden gibt Empfehlungen für die Durchführung von Penetrationstests (PeTe) auf IT-Systeme, -Applikationen und Netzen in der Bundesverwaltung. Es werden die Vorteile, aber auch die Grenzen eines PeTe aufgezeigt und ein Leitfaden für dessen Planung, Durchführung und Auswertung erstellt. Er richtet sich an die Entscheidungsträger im Informatikbereich bzw. Personen die mit der Durchführung eines PeTe beauftragt sind.

2. Allgemeines

Unter einem Penetrationstest versteht man den Versuch, autorisiert in ein Informationssystem einzubrechen, um Aufschluss über dessen Sicherheitsniveau zu erhalten. Oft fällt in diesem Zusammenhang auch der Begriff „Tiger-Team“.

Ziel eines PeTe können z.B. eine Firewall, ein Mail-, Web- oder Datenbankserver, Applikationen oder ganze Netze sein.

Oft werden solche Tests nach einer Installation von Sicherheitsmechanismen, wie beispielsweise einer Firewall, als Massnahme der Qualitätssicherung durchgeführt. Ziel ist die Erkenntnis, ob die Implementation den Sicherheitsanforderungen genügt. Grundsätzlich sollten Systeme im Rahmen eines Audits zuerst von „innen“ betrachtet werden, also eine Analyse und Härtung auf Systemebene bevor ein PeTe durchgeführt wird.

Ein PeTe ist nur dann sinnvoll, wenn bereits ein Sicherheitskonzept vorhanden ist. Mit einem PeTe wird dessen Umsetzung getestet und aufgrund der Ergebnisse ggf. angepasst. Von äusserster Wichtigkeit ist jedoch die Tatsache, dass ein PeTe, selbst wenn er Schwachstellen aufdecken sollte, grundsätzlich nicht geeignet ist, den Ist-Zustand eines Systemes festzustellen oder eine mögliche Bedrohung von aussen zu bewerten.

Vorhandene Schwachstellen können durch Penetrationstest nur teilweise gefunden werden.

Auch ein erfolgloser Eindringversuch zeigt nur, dass das System gegen diesen einen speziellen Angriffsversuch immun war. Ein neuer Versuch mit anderen Methoden könnte jedoch erfolgreich sein. Oft sind auch die verwendeten Werkzeuge nicht auf dem aktuellsten Stand. Ein PeTe birgt deshalb die Gefahr von Scheinsicherheit in

sich. Nicht zu unterschätzen sind auch die negativen psychologischen Auswirkungen auf die Administratoren der angegriffenen Systeme welche den PeTe als Misstrauensvotum interpretieren könnten.

Die Durchführung eines PeTe muss äusserst sorgfältig abgewogen, geplant und durchgeführt werden. Um den Einsatz sinnvoll und effektiv durchzuführen, sind umfangreiche und somit kostspielige Vorbereitungen nötig. Ohne sorgfältige Berücksichtigung der positiven Aspekte eines PeTe und die konsequente Vermeidung seiner negativen richtet ein PeTe u.U. mehr Schaden als Nutzen an.

Positive Aspekte eines PeTe:

- Aufdeckung einer Schwachstelle (falls erfolgreich)
- Kontrolle organisatorischer Massnahmen
- Funktionieren die Alarmmechanismen?
- Wie wird reagiert?
- Sensibilisierung der Verantwortlichen und des Managements (falls erfolgreich, ansonsten besteht die Gefahr von Scheinsicherheit beim Management)

3. Empfohlene Vorgaben und Vorgehensweise für PeTe

Voraussetzung für einen sinnvollen PeTe ist die im Voraus zu erstellende genaue Definition der Ziele, die durch den PeTe erreicht werden sollen. Die gesamte Vorgehensweise sollte genau geplant werden und mit den involvierten Personen besprochen werden. Zielsysteme, Netze und Applikationen werden vorgängig genau eingegrenzt. Es existiert ein Notfallprozedere für den Fall, dass Mensch und Systeme in unerwarteter Weise auf den Angriff reagieren (Ausfall von produktiven Systemen usw.). Während des PeTe sollten alle Aktionen genauestens und revisionsfähig protokolliert werden (Zeit, verwendete Tools, Zielsysteme, Resultate usw.). Werden während des PeTe weitere Schwachstellen entdeckt die nicht im ursprünglichen Fokus der Planung standen, so sollten diese zu einem späteren Zeitpunkt in einem eigens geplanten PeTe untersucht werden und nicht sofort im laufenden PeTe. Besteht die Möglichkeit, dass man während des PeTe auf sensitive Daten stösst (z.B. beim Sniffen in einem Netzwerk), so ist schon vorgängig der Datenschutzbeauftragte der Verwaltungseinheit (VE) oder des Bundes zu konsultieren. Alle Daten sind als vertraulich zu betrachten und entsprechen zu handhaben (siehe auch Punkt 4.5 Berichte).

3.1 Gefahrenanalyse

- Gefahrenanalyse des Systems
Wo sind bekannte oder mögliche Schwachstellen und wie wären die Auswirkungen eines allfälligen Angriffes durch Dritte? Wurde das System gemäss den Weisungen erhoben und die Massnahmen umgesetzt?
- Gefahrenanalyse für den PeTe selbst
Können Systeme während des PeTe ausfallen? Werden ungewollte

Konfigurationsänderungen an Systemen vorgenommen oder ungewollte Alarme ausgelöst?

Nach der Gefahrenanalyse wird ein GO/NoGO Entscheid für den PeTe gefällt.

3.2 Bestandesaufnahme des Systems vor dem PeTe

Wird dies unterlassen, kann später nur noch schwer nachvollzogen werden was durch den eigentlichen PeTe verändert wurde oder durch allfällige andere parallel arbeitende Angreifer verändert wurde (Backups!).

3.3 Planung des PeTe

Die Planungsphase umfasst die zu erwartenden Fachgebiete und Anforderungen, sowie die konkreten Zielfestlegungen. Weiter müssen die Rahmenbedingungen sowie die zum Einsatz kommenden Penetrations- und Auswertetools festgelegt werden. Es wird ein „Drehbuch“ für den Ablauf des Angriffes erstellt. Vor und nach der Planungsphase sollte ISB/SEC konsultiert werden. ISB/SEC ist bei der Planung gerne behilflich.

Angriffsart:	aktiv / passiv / andere Welche Systeme/Netze und Anwendungen sind Ziel des Angriffes?
Zeitplanung:	Tag / Uhrzeit – Beginn/Ende
Operative Planung:	Wer führt den PeTe durch? Ist ein Vertreter des Auftraggebers anwesend? Wer soll informiert werden? In welchen Räumlichkeiten findet der PeTe statt? Werden Benutzer-ID's, Ausweise und Batches benötigt?
Gefahren:	Produktionsausfälle, Schadensansprüche
Abbruchkriterien:	Beendigung nach welchen Erkenntnissen, Vorfällen usw. Der Auftraggeber muss jederzeit das Recht haben den PeTe vorzeitig abbrechen zu können.

Möglicher Stufenplan eines PeTe:

1. Informationsgewinnung
 - Kartographierung der Netztopologie
 - Analyse des Netzverkehrs
2. Physischer Zugriff auf die Netzwerkperipherie
 - Informationsgewinnung (z.B. mit Sniffer)
3. Logischer Zugriff auf Systeme im Netz
 - Informationsgewinnung und Analyse (Auf welchem System laufen welche Dienste? Gibt es bekannte Schwachstellen die ausgenutzt werden können?)
 - Versuch der Nutzung einer Schwachstelle
 - Eindringen in ein System
 - Analyse des Systemes von Innen (Falsch gesetzte Rechte im Dateisystem, trusted relationships zu anderen Systemen, Passwortanalysen etc.)
 - evt. Installation von Sniffern, Trojanern etc.

4. Weiteres Vordringen in andere Systeme aufgrund der gefundenen Informationen (gemeinsame Passwörter, trusted relationships)
5. Physischer Zugriff auf Systeme
6. Andere
 - Social Engineering etc. (ebenfalls Bestandteil des „Drehbuches“!)

3.4 Durchführung

Der Angriff sollte unter möglichst realen Bedingungen erfolgen. Das bedeutet, dass auf der Seite des Auftraggebers nur eine minimale Anzahl von Personen über den bevorstehenden Angriff informiert werden sollte. Somit ist z.B. auch gewährleistet, dass auch interne Alarmabläufe getestet werden können.

Das PeTe-Team versucht allfällige Schäden an Systemen möglichst gering zu halten.

Der Auftraggeber entbindet das PeTe-Team schriftlich von Schadensansprüchen. Liegt diese nicht vor, sollte kein PeTe durchgeführt werden! Davon ausgenommen sind jedoch Schäden die durch vorsätzliche oder grobfahrlässige Handlungen entstanden sind.

Es sollte immer eine neutrale Person (z.B. ISBO, ISBD, ISB/SEC) während des ganzen PeTe anwesend sein (Vieraugenprinzip).

Der Auftraggeber sollte das Recht haben, den PeTe jederzeit abbrechen zu dürfen.

Eine genaue Protokollierung der durchgeführten Aktionen, angegriffenen Systeme, verwendeten Tools, Änderungen an Systemkonfigurationen, Vorfälle usw. ist unerlässlich!

3.5 Bericht

Die Erstellung eines detaillierten Abschlussberichtes sollte vertraglich gefordert werden. Er verkörpert die vom Auftraggeber bestellte Dienstleistung. Im Bericht ist in ausführlicher und strukturierter Art auf die im PeTe erarbeiteten Ergebnisse einzugehen. Die Resultate werden von allen Beteiligten überprüft, abgesegnet und fließen in die Umsetzung der Schutzmassnahmen und Arbeitsabläufe ein. Deren Umsetzung kann ggf. mit einem weiteren PeTe oder Audit überprüft werden.

Der Bericht sollte mindestens enthalten:

- Zusammenfassung (Management Summary)
- Ziel / Aufgabenstellung
- Beteiligte Personen
- Ausgangslage
- Gewähltes Vorgehen
- Ablauf des PeTe (zeitlich, örtlich, Methoden usw.)

- Ergebnisse, geordnet nach Systemen, Netzen, Applikationen
- Empfehlungen
- Glossar

- Anhänge
 - Netzpläne
 - Protokolle des eigentlichen PeTe
 - Sitzungsprotokolle
 - usw.

Adressat für den Schlussbericht sind der Auftraggeber und die für die Zielsysteme zuständigen ISBO/ISBD. Die Übergabe des Schlussberichtes erfolgt in Papierform und/oder auf verschlüsselter CD-ROM gegen Quittung. Er sollte als **vertraulich** klassifiziert werden.

Die zuständigen Aufsichtsorgane erhalten, entsprechend den rechtlichen Grundlagen die ihre Tätigkeit regeln, eine Kopie oder die für sie relevanten Auszüge. Dabei ist der BRB vom Februar 2001 (Sicherheitsberichterstattung) strikte einzuhalten.

4. Wer erteilt den Auftrag für den PeTe und wer führt ihn durch?

Die Durchführung des PeTe sollte von der Direktion der betroffenen OE bewilligt und in Auftrag gegeben werden.

Sind durch den PeTe Systeme, Anwendungen, Daten oder Netze von mehr als nur einer OE betroffen sind (das dürfte der Regelfall sein!) sollte der A-IS vorgängig konsultiert werden.

Für den Auftraggeber ist oft nicht im Voraus klar, ob andere OE vom PeTe betroffen sind. Es ist deshalb wichtig, dass jeweils vor und nach der Planungsphase der zuständige ISBD sowie ISB/SEC mit einbezogen werden.

Wer führt den PeTe durch?

Es stellt sich die Frage wer vertrauenswürdige PeTe durchführt. Neben der Möglichkeit der Selbstdurchführung von Penetrationstests oder der Beauftragung der Hersteller- bzw. Lieferfirma des zu untersuchenden Informatiksystems ist vor allem der Einsatz von unabhängigen Spezialisten empfehlenswert (externe Firma oder eine unabhängige Fachstelle innerhalb des Bundes).

Allenfalls können die beigezogenen Personen vorgängig einer Sicherheitsprüfung unterzogen werden.

Anhang

Verwendete Abkürzungen und Begriffe

A-IS	A usschuss I nformatik s icherheit
BRB	B undesrats b eschluss
Firewall	Kontrollierter Netzwerkübergang zwischen eigenen und fremden Netzen
ISB/SEC	I nformatik s trategieorgan B und, Leistungsbereich Informatik s icherheit
ISBO	I nformatik S icherheitsbeauftragte/r der O rganisationseinheit
ISBD	I nformatik S icherheitsbeauftragte/r des D epartements
OE	O rganisation e inheit
PeTe	P enetration t est, das autorisierte Eindringen in Netze und Systeme
RVOG	R egierungs- und V erwaltungs o rganisations g esetz
Sniffen	Abhören des Netzwerkverkehrs
Social Engineering	Eine Vorgehensweise, mit der man unvorsichtiges Personal dazu verleitet oder überredet, Passwörter oder andere Informationen über Systeme und Netzwerke preiszugeben.
Trojaner	„Trojanisches Pferd“, eine Anwendung oder Code, der ohne Wissen des Benutzers heimlich und unautorisiert Aufgaben durchführt. Diese Aufgaben können die Systemsicherheit verletzen. Meist getarnt als „nützliches“ Hilfsprogramm.