

Datenschutzinfo – Einsatz von Sicherheitstools

Eine Info für IT-Leitung, IT-Administratoren und IT-Sicherheitsberater

Bekanntermassen ist der Einsatz bestimmter Sicherheitstools strafrechtlich nicht unproblematisch (§ 202 StGB – sog. Hackerparagraph).

BITKOM hat hierzu einen Leitfaden zur Bewertung und zum Einsatz von Sicherheits-Software und deren Funktionen herausgegeben.

Nachfolgend für Ihre praktische Tätigkeit ein Auszug aus dem Leitfaden.

Falls Sie Funktionen ausführen, die nachfolgend als kritisch dargestellt sind, sollten Sie weitere Abklärungen vornehmen und ggf. sich weiter absichern (z.B. über schriftl. Auftrag).

Software-Funktion	kritisch	unkritisch
Öffnen einer Kommandozeile auf dem angegriffenen Rechner zur Ausführung eines oder mehrerer Befehle	X	
Installation von Software zur Fernsteuerung oder nicht berechtigte Nutzung des angegriffenen Rechners	X	
Einbringen von eigenem Code durch den Angreifer / Angriffs-Software	X	
Ändern oder Löschen der Daten auf dem angegriffenen Rechner	X	
Auslesen der Daten auf dem angegriffenen Rechner	X	
Starten/Stören/Deaktivieren des angegriffenen Rechners oder seiner Dienste	X	
Angriff anderer Rechner bzw. Unterstützung oder Koordination solcher Angriffe	X	
Analyse von Software-Abläufen (Debugger, Disassembler)		X
Automatisierter Test von Software, um Verhalten im Fehlerfall zu dokumentieren (Fuzzer)		X
Passworte reproduzieren oder erraten	X	
Entschlüsselung von verschlüsselten Daten	X	
Änderung oder Einrichtung von Benutzerkonten und Änderung der Sicherheitskonfiguration	X	
Aufzeigen aktiver Geräte und Dienste im Netz (Portscanner)		X

Software-Funktion	kritisch	unkritisch
Aufzeigen von Sicherheitsschwachstellen im Netz oder in Applikation (Vulnerability-Scanner)		X
Selbstpropagierender Code (sich selbst weiter verbreitender Schadcode - Viren, Würmer, etc inkl. Baukästen)	X	
Umleiten von Netzwerkverkehr	X	
Mithören von Netzwerkverkehr	X	

Beispiel für Einsatz Passwort-Cracker

Funktionen	Bewertung
Passwörter reproduzieren oder erraten	Kritisch
Entschlüsselung von verschlüsselten Daten	Kritisch
Erläuterung	
Nach dem Bewertungsschema weist die Software klar Funktionen auf, die als kritisch anzusehen sind. Nur der Inhaber der Daten oder der Benutzer des Zugangs, für den das Passwort gebrochen wird, darf eine solche Maßnahme durchführen oder durchführen lassen.	

Unter Best Practice werden prinzipielle organisatorische Regeln für Unternehmen zum Einsatz von Sicherheitstools aufgeführt, u.a.

- Interne Sicherheits-Tests brauchen einen klaren Auftrag und einen klar definierten Personenkreis
- Sicherheitstools werden nur bestimmten Personen zur Verfügung gestellt
- Die Weitergabe von Passwörtern ist zu genehmigen oder ist in einer Aufgabenbeschreibung vorzugeben.
- Ergeben sich im Verlauf des Sicherheits-Tests die Möglichkeit zum Zugriff auf Daten Dritter, so darf auf die Daten nicht zugegriffen werden.
- Sicherheits-Tests für interne oder externe Kunden dürfen erst nach schriftlicher Beauftragung durch den Kunden begonnen werden, Umfang und Testdurchführung sind zu protokollieren.
- Tests, die Verhaltenskontrollen von Mitarbeitern oder Einsicht in deren private Daten ermöglichen, müssen genehmigt werden. In der Regel ist der BR einzubeziehen.

Weitere Ausführungen oder Erläuterungen finden Sie im Leitfaden von BITKOM „Praktischer Leitfaden für die Bewertung von Software im Hinblick auf § 202C, STGB, als Download erhältlich unter:

http://www.bitkom.org/de/publikationen/38337_52342.aspx

Für Rückfragen steht Ihnen auch Ihr Datenschutzbeauftragter zur Verfügung.

Georg Osner
Datenschutzbeauftragter

Georg.Osner@onlinehome.de
Tel: 0871-2760004