2011/36 dschungel

https://shop.jungle.world/artikel/2011/36/wikileaks-ausser-kontrolle

Skandal nach dem Skandal. Datenleck bei Wikileaks

Wikileaks außer Kontrolle

Von **Boris Mayer**

Schon im vergangenen Jahr hatten Kritiker von Wikileaks auf das mangelhafte Sicherheitskonzept der Whistleblower-Plattform hingewiesen. Der jüngste Datenskandal zeigt: Wikileaks kann die Informanten nicht schützen.

Nach dem »Cablegate«, wie die Veröffentlichung der US-Diplomatendepeschen durch die Enthüllungsplattform Wikileaks im vergangenen Jahr genannt wurde, haben wir nun das »Cablegate-Gate«. Seit vergangener Woche ist der bekannteste Whistleblower der Welt, Julian Assange, wieder in den Schlagzeilen, und erneut gibt es einen Skandal um Wikileaks. Dabei geht es nicht mehr um den Inhalt der geleakten Dokumente, sondern darum, dass durch die eigenmächtige Publikation die mit Klarnamen erwähnten Informanten gefährdet wurden.
Bereits im vergangenen Jahr sahen einige IT-Experten im geschlossenen System von Wikileaks Anzeichen dafür, dass man es bei der Whistleblower-Plattform mit der Sicherheit nicht ganz so genau nimmt. Bei den klar erkennbaren Mängeln handelte es sich zwar eigentlich nur um Kleinigkeiten, aber dass sie über Wochen und Monate nicht behoben wurden, obwohl dies einfach gewesen wäre, ließ befürchten, dass es um, von außen nicht sichtbare, dafür aber wesentliche Elemente des Sicherheitskonzepts von Wikileaks genauso schlecht stand.
Die Depeschen aus »Cablegate« sind nun in Form von unredigierten Originaltexten im Internet zu finden. In den ersten Tagen musste man noch das richtige Paket suchen und es dann aufwendig selbst entschlüsseln, inzwischen ist das nicht mehr nötig, man kann sich ein unverschlüsseltes Archiv herunterladen, wenn man denn weiß, wo man suchen muss.
Doch wie konnte es überhaupt passieren, dass diese Daten im Internet gelandet sind? Julian Assange, Daniel Domscheit-Berg, der ehemalige Sprecher von Wikileaks, und David Leigh von der britischen Zeitung Guardian schieben sich gegenseitig die Schuld zu.
Begonnen hatte alles, als Assange dem Journalisten Leigh das unredigierte Datenpaket mit den Depeschen zukommen lassen wollte. Assange packte alle Depeschen zu einer Datei zusammen und verschlüsselte diese dann mit dem Verschlüsselungsprogramm PGP. Die Abkürzung steht für Pretty Good Privacy. Ist eine Datei einmal mit PGP verschlüsselt, so benötigt man eine Passphrase, um die Daten wieder lesbar zu machen. Das nennt man symmetrische Verschlüsselung: Die Datei wird mit der gleichen Passphrase verschlüsselt, mit der sie auch entschlüsselt werden kann. Als Passphrase bezeichnet man ein langes Passwort. Bestehen die meisten Passwörter aus acht Zeichen, hat eine Passphrase eher die Länge eines ganzen Satzes. Normalerweise lässt man PGP diese Passphrase zufällig erstellen. Heraus kommt eine wirre Kette von Buchstaben, Zahlen und Sonderzeichen, die man sich nicht wirklich merken kann. Die

Passphrase wird dann einfach dem Dokument vorangestellt und asymmetrisch für die gewünschten Empfänger verschlüsselt. Dafür wird ein sogenannter Public Key verwendet. Nur wer den zu diesem öffentlichen Schlüssel gehörenden privaten Schlüssel besitzt, kann die Passphrase und somit die Datei entschlüsseln. Durch diese Methode kann jeder, der den Public Key einer Person kennt, Dateien für den Besitzer dieses Schlüssels verschlüsseln, doch nur der Besitzer des privaten Teils des Schlüsselpaares kann die Verschlüsselung auch wieder rückgängig machen. PGP verschlüsselt nur die Passphrase des eigentlichen Datenpakets asymmetrisch, weil so mehrere Empfänger hinzugefügt werden können, ohne dass das ganze Datenpaket für diese neu verschlüsselt werden muss.
Warum Assange auf die Möglichkeit verzichtete, eine Passphrase zu benutzen, die nur von Leigh hätte ausgelesen werden können, ist unbekannt. Als angeblich erfahrener Hacker hätte Assange eigentlich um das Verfahren wissen müssen. Stattdessen wurde eine Datei entstellt, die jeder entschlüsseln kann, der den zugehörigen Schlüssel kennt. Assange legte die verschlüsselte Datei in einem Verzeichnis auf den Webserver von Wikileaks, damit Leigh sie sich herunterladen konnte – und vergaß sie dann offenbar dort.
Von diesem Server konnte fortan jeder die Daten herunterladen, der das entsprechende Verzeichnis kannte. Und nicht nur das: Als der Webserver von Wikileaks in den Monaten nach der Veröffentlichung der Geheimdepeschen angegriffen wurde, wurde ein Backup aller Daten erstellt, die Wikileaks bis dahin erhalten und veröffentlich hatte. In einem Unterverzeichnis dieses Backup befand sich immer noch – unbemerkt von allen beteiligten Personen – das Depeschenpaket für den Guardian. Da man das Backup zur Sicherheit möglichst vielen Menschen zukommen lassen wollte, wurde es über Bittorrent verbreitet – und was einmal im Bittorrent-Netzwerk ist, lässt sich praktisch gar nicht wieder herausnehmen. Bittorrent ist ein Protokoll für die schnelle Verbreitung von großen Datenmengen an viele Personen und gehört zur Gruppe der Filesharing-Dienste.
Der nächste Fehler ist von Leigh gemacht worden. Er veröffentlichte die Passphrase in seinem im Februar erschienenen Buch »Wikileaks: Inside Julian Assanges War on Secrecy«. Assange hatte nämlich einen reißerischen Satz – ACollectionOfHistorySince_1966_ToThe_PresentDay# – gewählt, den er den Journalisten während eines Treffens aufgeschrieben hatte und in den noch ein mündlich weitergegebenes zusätzliches Wort eingefügt werden musste. Leigh ging nach eigener Aussage davon aus, dass die Passphrase längst nicht mehr benutzt wurde, weil ihm Assange dies versichert habe. Damit verstieß Leigh aber gegen eine der wichtigsten Regeln der Kryptographie: Verrate nie ein Passwort, auch wenn es schon ewig nicht mehr verwendet wird. Ein altes Passwort ist nämlich weit mehr als nur eine nicht mehr verwendete Buchstaben- und Zahlenkombination – es kann Hackern wertvolle Hinweise darauf geben, wie genau ein User es mit der Sicherheit nimmt und vor allem, zu welcher Art Codewort er neigt. Kennt jemand, der sich unberechtigten Zugang zu einem fremden Account verschaffen möchte, die Passwort-Gewohnheiten von dessen Inhaber, hat er leichtes Spiel, denn im schlimmsten Fall muss er nur noch fünf Prozent der eigentlich möglichen Passworte ausprobieren, um das aktuelle zu finden. Leigh wusste offensichtlich nicht, was er tat, als er das Passwort veröffentlichte, denn wie er in seinem Buch schrieb, schaffte er zwar die Entschlüsselung selbst, scheiterte aber an der Dekomprimierung der Daten, weil er das verwendete Programm 7zip nicht kannte. Er fuhr daraufhin zu Assange, um sich von ihm beim Entpacken helfen zu lassen – warum Assange dann nicht gleich die Daten persönlich übergeben hat, ist unklar.
Dass die Passphrase aus Leighs Buch nun mit der kursierenden Datei in Verbindung gebracht wurde, hängt wiederum mit dem Konflikt zwischen Assange und Domscheit-Berg zusammen, wegen dem letzterer Wikileaks verlassen hat. Bei Wikileaks gibt es seit Monaten keine

Möglichkeit mehr, Daten hochzuladen. Domscheit-Bergs Konkurrenzprojekt Openleaks hatte keinen guten Start. Er selbst wurde jüngst aus dem Chaos Computer Club ausgeschlossen, weil es wegen einer von ihm gewünschten CCC-Zertifizierung für Openleaks zum Streit kam – sein Hinweis an einen Journalisten der Wochenzeitung Freitag, dass das unzensierte Depeschenfile im Internet kursierte, brachte wiederum wohl Assange erst dazu, es nun zu veröffentlichen.