.BVT

CERT.at

GovCERT AUSTRIA

Erfahrungswerte aus den Webserver-Sicherheitsvorfällen von 2011

22.11.2011

Einleitung

Im Sommer und Herbst 2011 kam es zu diversen Einbrüchen bei bekannten Webseiten in Österreich. Es wurden sensible Daten kopiert und auszugsweise veröffentlicht, was zu einem erheblichen materiellen und auch immateriellen Schaden geführt hat. Das Team von CERT/GovCERT und Fachleute vom BVT waren an der Vorfallsbehandlung und Analyse aktiv beteiligt. Dabei stellte sich heraus, dass eine Reihe von Fehlern in der Betriebsführung diese Einbrüche begünstigt hatte.

Dieses Dokument basiert auf den bei diesen Einsätzen gesammelten Erfahrungen und will diese Lehren an alle Betreiber von Webservern in Österreich weitergeben, damit diese die Sicherheit ihrer Infrastruktur verbessern können. Die hier vorliegende Liste mit Empfehlungen ist kein umfassendes Handbuch und erhebt keinen Anspruch auf Vollständigkeit. Für eine erschöpfende Behandlung des Themas Sicherheit von Onlinediensten siehe etwa https://www.sicherheitshandbuch.gv.at/ oder andere entsprechende Fachliteratur.

Die folgenden Punkte sind daher primär als Denkanstoß und als Checkliste für Sofortmaßnahmen zu sehen, damit aus den Fehlern dieses Jahres gelernt werden kann und so weitere Einbrüche vermieden werden können.

Autoren:

Otmar Lendl mit Beiträgen aus dem BVT und dem Bundeskanzleramt.

Feedback:

Kommentare oder Rückfragen bitte an team@govcert.gv.at.

Inhalt

Administrative Fragen

Inventar

Unsere Erfahrung zeigt, dass sehr wenige Organisationen nur eine einzige Webseite (im Folgenden www.<organisation>.at genannt) betreiben, sondern dass die Zahl der Onlineauftritte überraschend hoch sein kann. Ein erster, notweniger Schritt ist daher, ein Inventar aller eigenen Webseiten zu erstellen. Dazu gehören:

- Die primären Webseiten
- Alle Webservices, die nicht für die Öffentlichkeit bestimmt sind, sondern die Dienstleistungen / APIs für andere Organisationen bereitstellen.
- Seiten, die für eine andere Organisation mitbetrieben werden (Dachverbände, …)
- Projektbezogene Webseiten
- Eventbezogene Webseiten (Konferenzen, …)
- PR/Marketing oder produktbezogene Seiten
- Entwicklungs/Testserver, alte oder noch nicht produktiv genommene Seiten

Extern gehostete Seiten

Bei einem Vorfall haben wir gesehen, dass die interne IT gut betreut und abgesichert war, aber eine der Webseiten extern betrieben wurde und deswegen nicht in das Sicherheitskonzept der Organisation eingebunden war.

Es ist nötig, auch in diesen Fällen eine zumindest administrative Sicherheitsverantwortung wahrzunehmen: die relevanten Verträge müssen klar definieren, wer für die Sicherheit zuständig ist, und wie überprüft werden kann, dass diese Verantwortung auch wahrgenommen wird.

Sicherheitsverantwortung Betriebssystem/Applikation/Inhalte

Sowohl bei im eigenen Haus betriebenen Webseiten, als auch bei extern gehosteten Seiten muss man sowohl den Aspekt „Sicherheit des Systems (Betriebssystem, Hardware-Management)“ als auch „Sicherheit der Applikation“ berücksichtigen. Gerade bei externem Hosting haben wir Fälle gesehen, wo Verträge für die Anwendung abgeschlossen wurden, das darunterliegende System aber außer Acht gelassen wurde. Oft geht der Auftraggeber davon aus, dass das System im Vertragsinhalt automatisch inkludiert ist, da dieses die Grundlage für die Anwendung ist.

Die Verantwortung für die Integrität der Inhalte der Webseite geht über die Absicherung des Webservers hinaus: Sind die Systeme, über die die Webapplikation gewartet und mit Inhalten gefüllt wird, auch hinreichend gesichert? (Beispiel: Schadsoftware am PC des Seitenbetreuers kann die Zugangsdaten zum CMS oder zum ftp-Zugang ausspähen und so zu einer manipulierten Webseite führen.)

Externe Dienstleister

Wie geht man mit den Zugängen von Dienstleistern um? Der Weg durch die Hintertür wird oft vergessen.

Regelmäßige externe Security Audits

Es hat sich gezeigt, dass Sicherheitsüberprüfungen von wechselnden, externen Dienstleistern ein unverzichtbarer Bestandteil einer erfolgreichen Sicherheitsstrategie sind.

Schon einfache Penetration-Tests hätten die Schwachstellen aufgedeckt, die zu den Einbrüchen des vergangenen Sommers geführt haben.

Neben dem Aufzeigen von technischen Schwachstellen eignet sich diese Maßnahme auch zur Überprüfung der organisationsinternen Fähigkeit, selbst nicht erfolgreiche Attacken zu erkennen. Typischerweise ist zumindest ein Zeitraum der Überprüfung bekannt; nutzen Sie externe Audits als Training der internen Eskalationsmechanismen.

Wer hat meine Daten noch?

In zwei Fällen wurden heuer Daten einer Organisation publik gemacht, die selbst nicht für den Verlust dieser Daten verantwortlich war. Für eine umfassende Datensicherheit sind daher folgende Fragen zu bedenken:

- Wem gebe ich regelmäßig Kopien von meinen Daten oder Zugang zu diesen? Wie gut ist dessen IT-Sicherheit und wie könnte ich verhindern, dass ein Einbruch beim Partner Effekte auf die eigene Organisation hat?
- Wer hat noch Datenbanken, die inhaltlich nahe an dem sind, was man selber verwaltet? Auch hier: Welche Öffentlichkeitswirkung hätte ein Datenleck dort?

Vorfallsmeldung

Oftmals werden Sicherheitsprobleme von wohlmeinenden Personen gefunden, die diese auch an die Verantwortlichen melden wollen. Solche Tipps sind sehr wertvoll und können einer Organisation bei entsprechender Behandlung spätere Einbrüche ersparen. Wird hingegen eine Warnung dauerhaft ignoriert, so kann das zu bösem Blut und öffentlichen Angriffen führen.

Wir empfehlen, die Annahme und Weitergabe von Sicherheitswarnungen in folgenden Bereichen sicherzustellen:

- Security-Kontakt auf Homepage
- Helpdesk / Hotline / Kundendienst. Sowohl per Telefon als auch per Email.
- Pressestelle
- Social Media (Facebook, Twitter, …)
- Auch alle andere Mitarbeiter: Weiß jeder MA, an wen er/sie sich melden kann, wenn er/sie etwas erfährt? Das kann auch völlig IT-Fremde treffen, die privat mit „Hey, du arbeitest doch bei XYZ. Weißt du, dass man ….“ angesprochen werden.

Medienstrategie

Im Falle eines Vorfalls ist es extrem wichtig, dass die Kommunikationsstrategie stimmt. Eine gelungene Medienarbeit kann viel Ärger ersparen. Dieses Dokument kann das Thema nur anreißen, etwa:

- Keine Zahlen nennen, die nicht wirklich gesichert sind.
- Keine Aussagen, die als Einladung zu weiteren Aktionen der Angreifer aufgefasst werden könnten.
- De-Eskalation in Richtung der Angreifer.
- Keine Aussagen über die Qualität der eigenen IT-Security („Wir haben eh alles gemacht“).
- Den Pressesprecher im Krisenfall reden lassen (der Geschäftsführer kann dann immer noch korrigieren.)

Technische Fragen

Mission Creep

Webseiten, die anfangs nicht wichtig und somit auch nicht besonders schutzbedürftig waren, können mit der Zeit weitere Funktionalitäten erhalten, die auch Änderungen in der Absicherung erfordern. Ein regelmäßiger Review der Sicherheitsrisiken und Gegenmaßnahmen ist daher nötig.

Interne Sicherheitstests

Die Tools, die von den Angreifern verwendet werden, sind großteils frei im Internet erhältlich und mit wenig Aufwand einsetzbar. Es spricht daher wenig dagegen, diese Tools einfach selber auf die eigene Infrastruktur anzusetzen.

Solche Tests sind nie ganz ohne Risiko, sie können Schäden oder Serviceunterbrechungen verursachen. Es ist aber oft nur eine Frage der Zeit, bis diese Tools von irgendwem im Internet gestartet werden, das lässt sich nicht verhindern. Es ist daher deutlich besser, wenn man diese Tests selber macht und sofort gegensteuern kann, als dass man wartet, bis sie ein böswilliger Angreifer von außen durchführt.

Angriffsfläche minimieren

Ein Webserver, der nur statische Files (HTML, PDF, Bilder) ausliefert, ist fast nicht angreifbar. Jedes weitere Feature vergrößert die Angriffsfläche. Aus dem Blickwinkel der Sicherheit ist hier Minimalismus angebracht, auch wenn das die Marketing- und PR-Abteilungen eventuell anders sehen.

Andere Webseiten/Applikationen am gleichen Server

Jeder weitere Virtual Host am gleichen Webserver kann ein Einfallstor für Angriffe auf die primäre Webseite sein. Ein „geben wir doch www.<irgendwas-anderes>.at auf unseren www.<organisation>.at drauf, dort haben wir noch Ressourcen“ ist gefährlich, außer diese weitere Seite wird genauso auf Sicherheitsprobleme getestet, wie die Hauptseite.

Zugriffe einschränken

Nicht alle Teile eines Webservers müssen vom ganzen Internet aus erreichbar sein. Insbesondere die Teile für die Verwaltung des Servers sollten zusätzlich auf IP-Adressbasis bzw. durch zusätzliche Konfiguration von Benutzernamen/Kennwort-Abfragen durch den Webserver unabhängig von der jeweiligen Anwendung (z.B. mittels htaccess-Dateien) eingeschränkt sein:

- Content-Management System (CMS)
  Falls dieses direkt in der operativen Domain betrieben wird, sollten die entsprechenden Pfade in der Webserver-Konfiguration abgesichert werden. Es reicht nicht, sich auf das User-Management des CMS zu verlassen.
- Web-basierte Administrations-Interfaces (phpmyadmin, cPanel, Plesk, …)
- ftp / sftp
  File-Uploads sollten nur von den notwendigen Adressbereichen aus möglich sein. Damit ist ein kompromittiertes User-Passwort nicht sofort für den Angreifer ausnutzbar.

Web Application Firewall (WAF)

Eine Web Application Firewall (im einfachsten Fall mod_security) kann eine weitere sinnvolle Komponente in der Verteidigungsstrategie sein, insbesondere im Notfall, wenn man die

Schwachstelle in der Applikation nicht schnell beheben kann. Eine WAF kann aber nie ein Ersatz für die sichere Programmierung von Applikationen sein.

Vorsicht ist auch dann geboten, wenn das organisationsinterne Netz an der WAF vorbei auf Webservices zugreifen kann.

Clean Server Policy

Analog zu einer „Clean Desk Policy“ (keine sensitiven Papiere am Schreibtisch liegen lassen), sollte man auf (Web-)Servern alle nicht gebrauchten Daten löschen. Dazu gehören:

- Temporäre Files
- Sicherheitskopien von Scripts („irgendwas.php.bak“)
- Datenbank-Dumps
- Files, die bei Debugging-Sessions angefallen sind
- Obsolete Applikationen und deren Daten(-banken)
- Transferdaten von und zum Server

Logging

Im Falle eines Einbruches ist es sehr hilfreich, wenn die Logfiles des betroffenen Servers vorhanden sind und diese vor Manipulationen geschützt waren. Ein Logging der sicherheitsrelevanten Events über das Netz auf einen (zentralen) Logserver kann hier besonders hilfreich sein.

Weiters ist es für die Analyse eines Vorfalls wichtig, dass alle beteiligten Geräte (Firewall, IDS, Webserver, …) synchronisierte Systemzeiten führen. Um im Falle einer Attacke die benötigten Informationen zur Hand zu haben empfiehlt es sich die Logging-Mechanismen bereits im Vorhinein auf den individuellen Informationsbedarf auszurichten. Hier wird ein Kompromiss zwischen Vollständigkeit und Handhabbarkeit der Daten getroffen werden müssen.

Google Hacking

In manchen Fällen waren es keine Einbrüche, die für Aufregung gesorgt haben, sondern schlicht Daten, die öffentlich auf Webservern abrufbar waren. Oft genug findet der die Suchmaschine Daten auf Webseiten, die dort abgelegt oder liegengelassen wurden, die aber nicht für die Öffentlichkeit bestimmt waren. „Google Hacking“ nennt man die Nutzung von Suchmaschinen zum gezielten Auffinden von Informationen, die entweder selber schon sensitiv sind, oder für echtes Hacking hilfreich sind.

Es ist daher ratsam, diese Informationsquelle selbst zu nutzen, um Datenlecks zu finden und zu beseitigen. Durch entsprechende Konfiguration des Servers kann schon die unerwünschte Indizierung bestimmter Bereiche weitgehend vermieden werden (Verwendung der Datei „robots.txt“) - Daten die von Suchmaschinen nicht indiziert wurden können auch nicht über diese gefunden werden.

Neustart nach einem Vorfall

Nachdem in einen Server eingebrochen und Inhalte verändert wurden, sollte man diesen Server vom Netz nehmen. Ein simples Richtigstellen der veränderten Information reicht bei weitem nicht.

Erst nach einer genauen Analyse und dem Beheben der Schwachstellen kann man daran denken, den Server wieder in Betrieb zu nehmen. Dazu gehört:

- Über welchen Weg ist der Angreifer ins System eingedrungen?

- Welche Daten wurden manipuliert / kopiert?
- Welche Privilegien hat sich der Angreifer verschaffen können?
- Konnte der Angreifer vom offensichtlich betroffenen System aus weitere kompromittieren?
- Sind alle im Zuge der Analyse entdeckten Schwachstellen gefixt?
- Findet eine aktive Suche nach weiteren Problemen auf dem Server nichts mehr?

Falls nicht ganz eindeutig klar ist, dass der Angreifer nur minimalen Zugriff erlangen konnte, ist eine komplette Neuinstallation des Systems angebracht. In diesem Zusammenhang sollte man auch bedenken, dass Angreifer oft bewusst offensichtliche Einbruchsspuren hinterlassen, um von den tatsächlich ausgenutzten Schwachstellen abzulenken um diese weiter zur Verfügung zu haben. Im Zweifelsfall sollte von einer vollständigen Kompromittierung ausgegangen werden.

Zusammenfassung

Die Sicherheitsvorfälle des Sommers und Herbst 2011 waren keine neuartigen Angriffe auf Webserver oder gar aufwändige, gezielte Attacken auf die komplette IT-Infrastruktur von Organisationen (Stichwort „Advanced Persistant Threat“ APT), sondern waren die Folgen von klassischen Fehlern in der Absicherung von Webservern.

Dieses Dokument soll als Checkliste für die Betreiber von Webseiten dienen, um schnell die wichtigsten Maßnahmen zur Absicherung dieser Dienste umsetzen zu können.

Diese Sofortmaßnahmen können aber kein dauerhafter Ersatz für eine durchdachte und gelebte IT-Sicherheitsstrategie innerhalb der eigenen Organisation sein.