THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

mein Alltag ist normiert! Mein Duschgel zeigt an, von der *Stiftung Warentest* geprüft worden zu sein, sogar die Note ist auf dem Etikett vermerkt. Der TÜV hat mein Fahrrad, das mich am Morgen schnell zum Bäcker trägt, auf Sicherheit geprüft, gemäß der EG-Öko-Verordnung wird der Belag für meine Backwaren abgesichert und auch meine Kaffeemaschine unterliegt Normen und Grenzwerten.

Die Vorteile dieser standardisierten Prüfverfahren, die diese und viele andere Produkte durchlaufen müssen, liegen auf der Hand:

- Normierte Vorgehensweise
- Linear abzuarbeitender Prüfkatalog
- Abweichungen zwischen Norm und Befund sind auffällig
- Reproduzierbare, (rechtlich) verbindliche Ergebnisse

Auch für komplexe Systeme existieren Prüfstandards. Diese definiert der VDE (VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.) folgendermaßen: „Prüfen elektrischer Anlagen beschreibt das Sicherstellen der Funktion und Sicherheit mittels geeigneter Prüf- und Messverfahren nach dem Errichten, Erweitern oder Ändern solcher Anlagen“.

Summa summarum – Standards mit Normen, Richt- und Grenzwerten bieten mehr Komfort und Sicherheit sowie Verlässlichkeit für den Verbraucher.

Seitens der Industrie höre ich immer wieder den Wunsch nach einem standardisierten Penetrationstest, der vergleichbare, reproduzierbare Ergebnisse hervorbringt. Vor strikt standardisierten Penetrationstests jedoch möchte ich warnen. Penetrationstests stellen zwar ebenfalls Prüfverfahren dar – allerdings unter außergewöhnlichen Rahmenbedingungen:

1. Der Untersuchungsgegenstand liegt in einem äußerst dynamischen Umfeld:
   a) Angriffs-Tools entwickeln sich rapide weiter
   b) Der Prüfgegenstand wandelt sich stetig
   c) Der Prüfkatalog wird ständig aktualisiert
2. Nicht-lineares Vorgehen und Interdependenzen: Jeder nächste Teilschritt eines Penetrationstests hängt vom Resultat des vorhergehenden ab
3. Abstraktionsvermögen für Perspektivwechsel

(Fortsetzung auf der nächsten Seite)

Bitte beachten Sie die Hinweise zu unserem Whitepaper und unserer Incident-Response-Notfallnummer auf der nächsten Seite

Aktuelle Events

Vortrag auf dem Seminar „Sicheres Mobile Computing“

23.07.13	in Köln
23.08.13	in München
27.09.13	in Frankfurt/Main
24.–26.09.13	LH[1] auf der Landesmesse Stuttgart: IT+Business
08.–10.10.13	LH[1] auf it-sa 2013

[1] Live Hacking

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

WLAN: 10. - 11.09.13	**Exploits:** 01. - 02.10.13
IT-Security I: 16. - 17.09.13, 21. - 22.10.13, 25. - 26.11.13	**Incident Response:** 15. - 17.10.13
IT-Security II: 18. - 19.09.13, 23. - 24.10.13, 27. - 28.11.13	**IT-Forensik:** 05. - 07.11.13
PenTests: 23.09.13, 15.11.13	**Mobile Device:** 12. - 13.11.13
Web-App: 25. - 26.09.13, 20. - 21.11.13	**IT-Recht:** 29.11.13
	Windows-Angriffe: 03. - 04.12.13
	IPv6: 06.12.13

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit, wir werden Sie dann umgehend aus dem Verteiler entfernen.

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Marcus Bauer

THE PENTEST EXPERTS.

Wenn ich mit Gartengerät dem Wildwuchs Herr werden möchte, bin ich froh um die Vorteile von Grenzwerten und normierten Prüfverfahren, die mir die Sicherheit geben, dass die Gerätschaft nicht mich trimmt, sondern den Rasen und Garten. Die Kreativität in einem dynamischen und sich sehr schnell verändernden Feld, wie dem des professionellen Hackings, zu beschneiden, könnte jedoch fatale Folgen haben.

Wir empfehlen daher, all das zu standardisieren, was sich gut standardisieren lässt: die Eingrenzung des Prüfgegenstands, des Prüfzeitraums, der Angriffsperspektive und der Prüfmethodik. All das erfolgt in Absprache mit dem Kunden anhand einer Checkliste mit Protokoll. Ein Minimalvorgehen wie beispielsweise der Einsatz eines bestimmten Scanners lässt sich ebenfalls definieren. Darüber hinaus muss aber der Penetrationstester genug Freiheit besitzen, um dieselbe Kreativität entfalten zu können, wie dies auch ein Hacker tut.

Herzliche Grüße,
Ihr Sebastian Schreiber

Neues Whitepaper:

Wir haben unser Whitepaper von Grund auf aktualisiert und überarbeitet. Wenn Sie eine Kopie (als PDF oder gedruckt) wünschen, so zögern Sie nicht, sich ein Exemplar über info@syss.de anzufordern.

Gehackt? Fremdeinwirkung? Daten gestohlen?

Sollten Sie den Verdacht hegen, in Ihr IT-System könnte eingedrungen worden sein, so zögern Sie nicht, sofort mit uns in Kontakt zu treten.

Wir haben eine **Incident-Response-Notfallnummer** eingerichtet: **+49 (0)7071 - 407856-99**.

Lifestyle oder Datensicherheit – Muss der Nutzer sich entscheiden?

von Matthias Dettling und Kim Unger

Die Vermessung der Welt – ein Roman von Daniel Kehlmann, beschreibt eigentlich die Geschichte zweier Berühmtheiten – trifft aber ebenso auf die ein jeden umgebende moderne Lebenswirklichkeit zu.

Und es hätte die beiden Romanhelden den Mathematiker Carl Friedrich Gauß und den Wissenschaftler Alexander von Humboldt nicht Wunder genommen, dass der Mensch des 21. Jahrhunderts nicht nur die Welt, sondern vor allem auch sich selbst vermisst.

Smart Body Analyzer, Jawbone UP und FitBit One – so heißen die Selbst-Vermessungsinstrumente zu mehr Überblick und Kontrolle des eigenen Körpers und Gesundheitszustands. Das Datenspektrum, das von den Geräten abgedeckt wird, ist dabei vielfältig. Sie messen Schlafverhalten, Distanz, verbrannte Kalorien, Dauer und Intensität einer Aktivität.

Der Smart Body Analyzer des Herstellers Withings misst Gewicht, Körperfett, Herzfrequenz und CO2-Gehalt in der Luft. Unsere Untersuchungen haben jedoch gezeigt, dass nicht immer wir selbst die Einzigen sind, die unseren Körper überwachen und bisweilen nehmen wir mit fremder manipulativer Hilfe schnell an Gewicht zu.

Gemein ist allen Körpervermessungsinstrumenten, dass die erhobenen Daten auf eine Onlineplattform übertragen werden, eine visuelle Aufbereitung der Daten erfolgt aber auch einfach mithilfe einer App. Die erfassten Daten gelangen je nach Produkt beziehungs-

weise Konfiguration auf unterschiedlichen Wegen in die Onlineplattform des Herstellers. Der Smart Body Analyzer kann sowohl direkt über WLAN mit der für die Datendokumentation bereitgestellten Onlineplattform kommunizieren als auch über Bluetooth mit einem Smartphone, das die Daten dann an die Applikation und von dort an Withings überträgt, falls kein WLAN zur Verfügung steht.

Kritisch ist, dass beide Kommunikationswege lediglich über HTTP – also unverschlüsselt – verlaufen. Auch die Smartphone-App, welche die Daten an die Withings-Plattform sendet, überträgt diese unverschlüsselt.

Da auf Verschlüsselung verzichtet wird, ist es einem Angreifer möglich, den Netzwerkverkehr zwischen Waage und Server oder zwischen App und Server abzuhören und auch darauf Einfluss zu nehmen. Ein Angreifer, der lediglich auf der Leitung lauscht, kann beispielsweise das aktuelle Gewicht aller Benutzer der Waage mitlesen. Dasselbe gilt für die Raumtemperatur und den CO2-Gehalt sowie alle weiteren Daten, die von der Waage an den Server übermittelt werden.

Für die Benutzerauthentifizierung wird ein Hash-Verfahren (MD5) verwendet, das von der SySS GmbH schon seit Jahren nicht mehr empfohlen wird. Ein Angreifer könnte die in einer abgehörten Anmeldung enthaltenen Daten nutzen, um das Passwort zu errechnen.

Eine technische Erweiterung der Lifestyle-Überwachungsgeräte ist zum Beispiel denkbar mit der Ergänzung durch die eigenen Geodaten, anhand derer man erkennen kann, ob ein Tag eher minderer Leistungsfähigkeit beeinträchtigt war von Pollenflug. Der gemessene Mensch wäre dann auch noch trackbar. Doch auch mit den üblichen Funktionen sind diese Daten nicht unerheblich.

Quelle: SySS GmbH

Der Schutz dieser Informationen auf dem Transportweg könnte durch technische Mittel sichergestellt werden. HTTPS anstatt HTTP zu verwenden, könnte neben der Vertraulichkeit und Integrität weiterhin die Authentizität des Kommunikationspartners gewährleisten. Dass jedoch gesundheitsrelevante Informationen in die Hände Dritter gelangen, ist das eigentliche Problem bei der Nutzung dieser Lifestyle-Produkte. Zur Nutzung der Dienste wird hier gewöhnlich vom Nutzer gefordert, die Bestimmungen zum Datenschutz zu bestätigen, die ihrerseits wiederum bestätigen, dass das Recht an den eigenen Daten nun beim Anbieter liegt. Eine Zweitverwertung der Daten ist somit denkbar. Interessant könnte das für Krankenkasssen, Versicherungen und Arbeitgeber sein. Über diese Datenspionage könnten sie erfahren, wie der aktuelle Gesundheitszustand von Patienten, Klienten oder Mitarbeitern ist.

Auf den Nenner gebracht, wer sehr persönliche Daten für sich allein haben will, der sollte den Einsatz solcher Geräte überdenken. Ein Anbieter, der vertrauensvoll mit den Daten der Nutzer umgeht, wird nicht mithilfe der Datenschutzerklärung dem Nutzer die Rechte an eigenen Daten absprechen, um sie so für eine Zweitverwertung vorzubereiten. Daten sollten verschlüsselt gespeichert werden, der Schlüssel würde auf Seiten des Kunden verbleiben und den Anbieter von jeglicher Einsichtnahme ausschließen. Zum jetzigen Zeitpunkt muss der Nutzer bei diesem Gesundheitscheck viel Vertrauen haben, denn Kontrolle hat er nicht.