GIBT ES EVIDENZBASIERTE IT-SICHERHEIT?

Hanno Böck
https://hboeck.de

EMPFEHLUNGEN IN SACHEN IT-SICHERHEIT

INSTALLIERT EIN ANTIVIRENPROGRAMM!

Virenschutzprogramme

Wie Sie bereits wissen, ist ein Virus für Ihren PC so ähnlich wie für Sie eine Grippe. Nur, dass Sie Ihren Rechner nicht zum Arzt bringen müssen. Wichtiger ist vielmehr, ihn vor der Infektion zu schützen. Das können Sie tun, indem Sie ein Anti-Viren-Programm oder Viren-Scanner installieren. Unter Windows ist eine gute Antiviren-Software unerlässlich, da Windows-Rechner aufgrund ihrer weiten Verbreitung am häufigsten angegriffen werden Für Linux und MAC OS X sind bislang kaum Schadprogramme bekannt, die „kommerziell“ genutzt werden. Ein Programm zum Schutz des eigenen Rechners ist daher bei privater Nutzung des Rechners nicht zwingend notwendig, aber dennoch empfehlenswert, um nicht versehentlich gefährliche Dateien an andere weiterzugeben.

Quelle: BSI

DEINSTALLIERT EUER ANTIVIRENPROGRAMM!

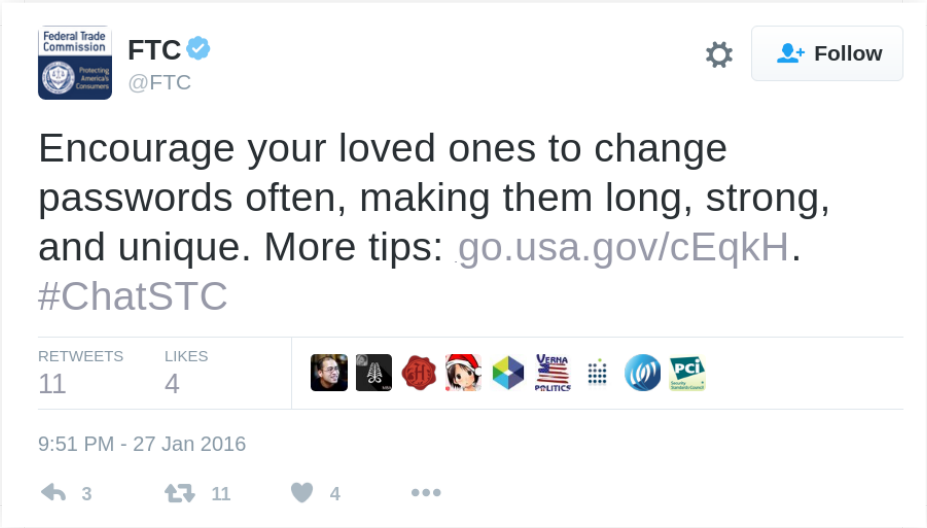
THURSDAY, 26 JANUARY 2017

Disable Your Antivirus Software (Except Microsoft's)

I was just reading some Tweets and an associated Hackernews thread and it reminded me that, now that I've left Mozilla for a while, it's safe for me to say: **antivirus software vendors are terrible; don't buy antivirus software, and uininstall it if you already have it (except, on Windows, for Microsoft's)**.

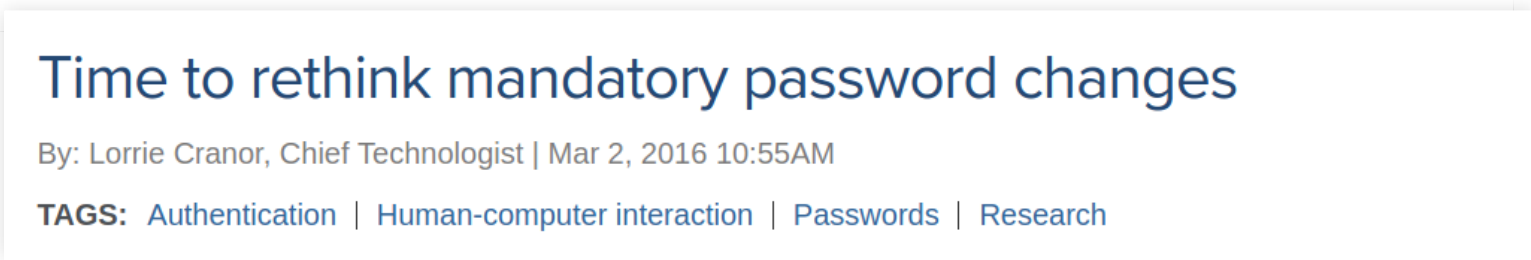
Robert O'Callahan, ehemaliger Mozilla-Entwickler.

PASSWÖRTER REGELMÄSSIG WECHSELN!



Quelle: FTC

PASSWÖRTER NICHT REGELMÄSSIG WECHSELN!



Quelle: FTC

WISSENSCHAFT

Sollten wir Entscheidungen - auch in Sachen IT-Sicherheit - nicht auf wissenschaftlicher Basis treffen?

WISSENSCHAFT

PSYCHOLOGIE

"SOCIAL PRIMING"

ALTER / GESCHWINDIGKEIT

Experiment: TeilnehmerInnen werden Worte vorgelegt, sie sollen daraus Sätze bilder.

Ergebnis: TeilnehmerInnen, die vorher Sätze mit Bezug zu Alter erhielten, laufen anschließend langsamer.

Reconstruction of a Train Wreck: How Priming Research Went off the Rails

February 2, 2017 Kahneman, Priming, r-index, Statistical Power, Thinking Fast and Slow

Authors: Ulrich Schimmack, Moritz Heene, and Kamini Kesavan

"FILE DRAWER PROBLEM" ODER PUBLICATION BIAS

SCHLECHTE STUDIEN FÜR ANFÄNGER

1. Suche eine interessant klingende, aber unsinnige Theorie.
2. Führe Studie durch, die Theorie bestätigt.
3. Wenn Theorie bestätigt wird: Publizieren. Andernfalls: Papierkorb.
4. Andernfalls: Zurück zu Schritt 2.

Bei p-Wert von 0,05 im Schnitt 20 Studien nötig für signifikantes Ergebnis.

SCHLECHTE STUDIEN FÜR FORTGESCHRITTENE

1. Suche eine interessant klingende, aber unsinnige Theorie.
2. Führe Studie durch, die Theorie bestätigt.
3. Falls Ergebnis nicht signifikant: Andere

> "The conventional view of the research process is that we first derive a set of hypotheses from a theory, design and conduct a study to test these hypotheses, analyze the data to see if they were confirmed or disconfirmed, and then chronicle this sequence of events in the journal article. (...) But this is not how our enterprise actually proceeds. Psychology is more exciting than that (...)" (Bem, 2000, p. 4).
>
> "To compensate for this remoteness from our participants, let us at least become intimately familiar with the record of their behavior: the data. Examine them from every angle. Analyze the sexes separately. Make up new composite indexes. If a datum suggests a new hypothesis, try to find further evidence for it elsewhere in the data. If you see dim traces of interesting patterns, try to reorganize the data to bring them into bolder relief. If there are participants you don't like, or trials, observers, or interviewers who gave you anomalous results, place them aside temporarily and see if any coherent patterns emerge. Go on a fishing expedition for something–anything–interesting." (Bem, 2000, pp. 4-5)

Bem (2000), in Wagenmakers, Wetzels, Borsboom, van der Maas (2011)

J Pers Soc Psychol. 2011 Mar;100(3):407-25. doi: 10.1037/a0021524.

Feeling the future: experimental evidence for anomalous retroactive influences on cognition and affect.

GEGENWIND

- Replication Bullies
- Research Parasites
- Replication Terrorists

OSF REPRODUCIBILITY PROJECT

GEGENMASSNAHMEN

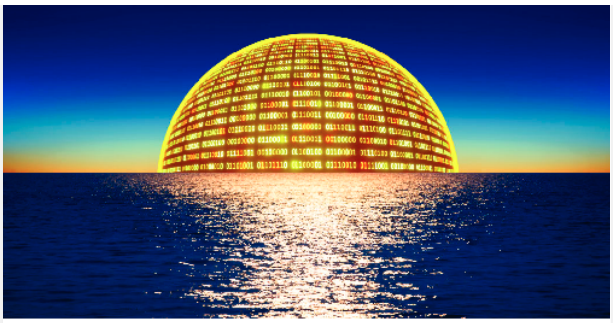
- Studien replizieren, negative resultate publizieren.
- Studienregister, registered reports (Methoden publizieren und im Idealfall Publikationsentscheidung treffen bevor Daten gesammelt werden).
- Standardisierte / bessere statistische Methoden, höhere Signifikanzschwellen, Daten und Code mitveröffentlichen.

WISSENSCHAFT

Die Mehrzahl der wissenschaftlichen Resultate ist falsch.

"Studien" alleine reichen nicht. Wir müssen nach methodischer Qualität und möglichen Fehlerquellen fragen.

ZERO DAYS



Zero Days, Thousands of Nights

The Life and Times of Zero-Day Vulnerabilities and Their Exploits

Lillian Ablon, Andy Bogart

RAND CORPORATION

"This report provides really valuable analysis and, crucially, cold hard data into a debate that often runs on base assertions and anecdotes, rather than statistical evidence and analysis," Matt Tait, the founder of Capital Alpha Security, and a former information security specialist for GCHQ, told Motherboard in an email.

Die Rand-Studie bietet bislang einmalige Einblicke in das Ökosystem der 0days in ihrem natürlichen Lebensraum. Die Rand Corporation wird zwar von der US-Regierung gefördert, hat sich aber einen Ruf als unabhängige Organisation erarbeitet, den auch diese Analyse bestätigt. Die Studie hinterlässt einen sehr seriösen Eindruck. Dazu trägt unter anderem bei, dass die Autoren an mehreren Stellen die Aussagekraft der Daten beziehungsweise die Validität der eigenen Aussagen kritisch hinterfragen.

"COLD HARD DATA"

Klingt fast wie Wissenschaft.

KOLLISSIONSRATE VON ZERO-DAYS

Wer einen Zero-Day besitzt, weiß nicht, ob andere bereits Informationen über die selbe Sicherheitslücke haben. Relevant für Risikoeinschätzung.

RAND-Report: 5 Prozent Kollissionsrate.

DATEN

"We believe these data are relatively representative of what a sophisticated nation-state might have in its arsenal."

DATENHERKUNFT

Unbekannte Firma, die im Report "BUSBY" genannt wird.

PROBLEME RAND-REPORT (1)

- 20 - 30 Bugs wurden entfernt ("due to operational..."). Filterkriterien? Unklar.
- Waren 207 + 20-30 Bugs alle Sicherheitslücken, die BUSBY besaß? Unklar.
- Warum sollen wir glauben, dass BUSBY repräsentativ ist? Unklar.

PROBLEME RAND-REPORT (2)

- Daten? Welche Daten eigentlich? Der Report enthält nur Schaubilder und Tabellen, aber keine Rohdaten.
- Unter welchen Bedingungen wurden die Daten geteilt? Hatte BUSBY am Report mitgearbeitet? Möglicherweise sogar ein Publikationsveto gehabt? Unklar.

INTERESSENSKONFLIKT?

PUBLICATION BIAS?

BUSBY hat die Daten freiwillig geteilt.

Welche Daten hat BUSBY geteilt? Hat RAND andere Akteure angefragt, die vergleichbare Datensätze verfügbar haben?

KOLLISSIONSRATE

For a given stockpile of zero-day vulnerabilities, after a year, approximately 5.7 percent have been discovered by an outside entity.

MOMENT...

Wir wissen weder, wie viele Akteure es gibt, noch, wie viele Bugs die jeweiligen Akteure besitzen.

Die Kollissionsrate von 0days könnten wir nur berechnen, wenn wir Kenntnis über alle 0days von

KOLLISSIONSRATE

Ideally, we would want similar data on Red (i.e., adversaries of Blue, or other private-use groups), to examine the overlap between Blue and Red, but we could not obtain that data. Instead, we focus on the overlap between Blue and the public (i.e., the teal section in the figures above) to infer what might be a baseline for what Red has. We do this based on the assumption that what happens in the public groups is somewhat similar to what happens in other groups. We acknowledge that this is a weak assumption, given that the composition, focus, motivation, and sophistication of the public and private groups can be fairly different, but these are the only data available at this time.

"WEAK ASSUMPTION"?

Anders ausgedrückt:

"Wir wollten eigentlich die Kollissionsrate von unbekannten 0days bestimmen. Da wir das nicht konnten haben wir eine völlig andere Frage

TESTS VON IT-SICHERHEITSPRODUKTEN

41

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO For

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Securi

Mobile Security | Wireless Security

Home › Network Security

Sophos Blasts Cylance's Competitive Testing Methods

By Kevin Townsend on June 30, 2016

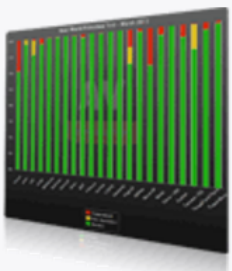
Share 348 | G+1 6 | Tweet | Recommend 23 | RSS

Real-World Protection Tests

This section contains full product long-term dynamic test reports. These tests evaluate the suites “real-world” protection capabilities with default settings (incl. on-execution protection features). It is our aim to do these tests rigorously. Due to that, these tests are time and resource expensive, so only products chosen for the yearly main test-series are included. Results are released monthly, together with two overview reports (July and December).

Our award-winning Real-World Protection Test framework has been recognized by the **“Standortagentur Tirol”** with the 2012 “**Cluster Award for innovation in computer science”** and by the **“Austrian Government”** with the 2013 **“Constantinus Award”**.

Beside the animated charts we have very extensive reports. Please have a look at them.



"REAL WORLD PROTECTION TEST"

Klingt fast so als würde hier unter realen Bedingungen getestet. Ist aber nicht so.

"INDEPENDENT"

There was much debate as to how to support AV-Comparatives without compromising its most important quality, namely its neutrality. Payment must not be allowed to have any influence on test results.

The solution actually turned out to be very simple: if all manufacturers pay the same fee in order for their product to be tested, none of them can be advantaged or disadvantaged. In several cases it happens that a vendor is tested even if it do not apply for it. In this case, the costs will be covered either by the magazines or by other independent parties, which

AV-TESTS

Es gibt eine ganze Branche von AV-Testfirmen und Organisationen.

Fast alle werden aus der Antiviren-Branchen selbst finanziert.

Niemand tested mit realen Nutzern.

WIE WÜRDE MAN ES RICHTIG MACHEN?

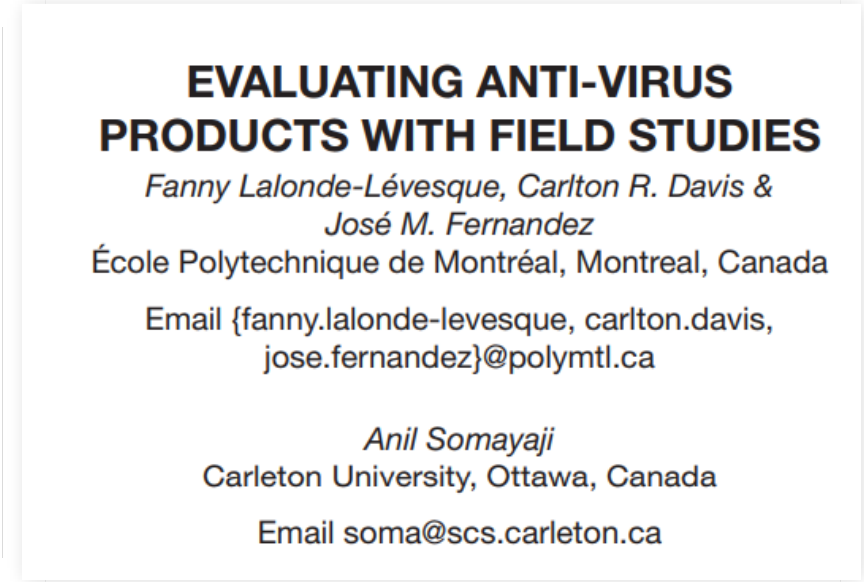
MEDIZIN: RCTS

- RCT (Randomized controlled trial)
- Teilnehmer in mehrere Gruppen unterteilen (Beispiel: neues medikament, altes Medikament, Alternative zum Medikament wie bspw. Erährungsumstellung, Placebo-Kontrollgruppe).
- Wenn möglich verblinden.

KEINE EINZELSTUDIEN

- Studien müssen repliziert werden.
- Metaanalyse - Zusammenfassung mehrere Studien.
- Auch hier: Problem Publication Bias - kenne ich alle Studien?

Das war eine vollständige auflistung aller RCTs zu Antivirenprogrammen und anderen IT-Sicherheitsprodukten.



EVALUATING ANTI-VIRUS PRODUCTS WITH FIELD STUDIES

Fanny Lalonde-Lévesque, Carlton R. Davis & José M. Fernandez
École Polytechnique de Montréal, Montreal, Canada

Email {fanny.lalonde-levesque, carlton.davis, jose.fernandez}@polymtl.ca

Anil Somayaji
Carleton University, Ottawa, Canada

Email soma@scs.carleton.ca

FTC UND PASSWÖRTER (1)

Im Januar 2016 verschickte die FTC einen Tweet, in dem sie das regelmäßige Wechseln von Passwörtern empfahl.

Lorrie Cranor von der FTC machte sich auf die Suche

das Gegenteil.

FTC UND PASSWÖRTER (2)

Gut: Die FTC fragt nach wissenschaftlichen Belegen.

Eher schlecht: Alle von der FTC angeführten Studien sind von eher schwacher Aussagekraft. Sie basieren alle auf Modellen oder Beobachtungsdaten (Korrelation != Kausalität).

FAZIT

Die Debatte um wissenschaftliche Qualitätsstandards (Replikationen, Studienregister etc.) findet momentan in der Informatik und der IT-Sicherheitsforschung praktisch nicht statt.

oder nur wenige, qualitativ miserable wissenschaftliche Belege.

Wir brauchen evidenzbasierte IT-Sicherheit auf Basis qualitativ hochwertiger Wissenschaft.