Der Blick in die Medien

protekto
Für den Menschen

Merkurist. mainz

News Snips

CYBERKRIMINALITÄT

Polizei Mainz warnt vor großem Anstieg von Hacker-Angriffen

Die Cyberkriminalität in Rheinland-Pfalz hat zugenommen. Durch Hackerangriffe können persönliche Daten veröffentlicht werden, auch Energieversorgung und medizinische Einrichtungen sind gefährdet. Was unternehmen Polizei und LKA gegen Hacker?

Mehr als tausend Firmen weltweit haben Kriminelle kürzlich durch einen Angriff auf eine amerikanische IT-Firma lahmgelegt. Sie hatten die Software durch ein Erpressungsprogramm manipuliert und so die Unternehmen verschlüsselt, die Firmen konnten also nicht mehr auf ihre Daten zugreifen. Das hatte Auswirkungen bis nach Europa: In Schweden etwa mussten daraufhin 800 Filialen der Supermarktkette Coop schließen.

---

mdr.de

Nach Attacke auf Kreis Anhalt-Bitterfeld

Vorlesen

LKA rechnet mit hoher Dunkelziffer bei Cyber-Angriffen

von MDR SACHSEN-ANHALT

Stand: 08. Juli 2021, 16:19 Uhr

Nach der Cyber-Attacke auf die Verwaltung des Landkreises Anhalt-Bitterfeld geht das Landeskriminalamt von einer hohen Dunkelziffer in anderen Bereichen aus. 2020 gab es allein in Sachsen-Anhalt wöchentlich rund 290 Anzeigen wegen Cyber-Kriminalität.

Nach dem Angriff auf die Kreisverwaltung in Anhalt-Bitterfeld ist offenbar auch in anderen Bereichen von einer hohen Dunkelziffer an Cyber-Attacken auszugehen. Der Sprecher des Landeskriminalamtes (LKA), Michael Klocke, sagte MDR SACHSEN-ANHALT, die Dunkelziffer sei garantiert erschreckend. Im Zusammenhang mit Cyber-Crime im weiteren Sinne habe es im vergangenen Jahr rund 290 Strafanzeigen pro Woche gegeben. Das sei enorm.

Klocke ergänzte, Cyber-Angriffe auf Behörden und Ämter in Sachsen-Anhalt seien bisher aber die absolute Ausnahme. Der Angriff auf den Landkreis Anhalt-Bitterfeld sei allerdings auch kein Einzelfall. Kriminelle versuchten hier, bestehende Sicherheitslücken zu nutzen.

---

internetworld.de

Themen Events Magazin Stellenmarkt Newsletter plus Podcast Video

SECURITY plus 25.07.2021

Cybercrime im E-Commerce

Die 5 häufigsten Angriffe auf Online Shops - und Tipps zur Vermeidung

Quelle: shutterstock.com/Rawpixel.com

Dem E-Commerce gehen weltweit jährlich Milliarden von US-Dollar durch Cybercrime verloren. Wir erläutern die wichtigsten Bedrohungen, mit denen Unternehmen im E-Commerce konfrontiert sind, und erklären, wie man sowohl den Webshop als auch Kunden besser schützen kann.

---

pcwelt.de

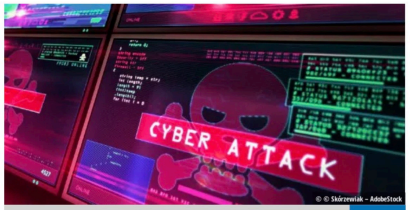
PCWELT SICHERHEIT powered by Norton

Home > Computer & Technik > Sicherheit > Antivirus & Firewall 1768268

Die 10 gefährlichsten Internetangriffe

14.07.2020 | 13:02 Uhr | Roland Freist

Täglich zählen die Security-Anbieter Tausende von neuen Viren und Angriffsmethoden. Doch am bedrohlichsten sind die Attacken, die technisch besonders fortgeschritten sind. Mit Know-how sowie unseren Tipps und Tools schützen Sie sich.



Schaut man sich die Liste namhafter Schädlinge aus dem Internet an, hat man einiges zu lesen. Wir stellen die typischsten Gefahren vor.

© © Skórzewiak – AdobeStock

Vergrößern

---

tagesspiegel.de

DER TAGESSPIEGEL SUCHE

Schwere Internet-Störung auf Nachrichtenseiten

UPDATE 22.07.2021, 18:55 Uhr

Mehrere deutsche Webseiten down

Einige deutsche Webseiten waren von einer Störung betroffen. Sie waren für Nutzer nicht erreichbar.

Riesige Störung

Viele deutsche Internetseiten nicht erreichbar - auch FOCUS Onlin betroffen

Liebe Leser, aufgrund technischer Probleme sind derzeit viele Internetseiten in Deutschland größtenteils nicht funktionsfähig. Dazu z… auch unsere Marken FOCUS Online, Bunte und Chip. Wir versuchen, die Probleme so schnell wie möglich zu beheben. »

Das Nachrichtenportal informiert auf seine Seite über die Störung. FOTO: SCREENSHOT TAGESSPIEGEL

Nach der Störung bei einem Internet-Dienstleister sind am Donnerstag diverse Websites zeitweise nicht erreichbar gewesen. In Deutschland etwa konnten am späten Nachmittag unter anderem Seiten von RTL und „Focus" nicht aufgerufen werden. Der Web-Dienstleister Akamai hatte zuvor Probleme bei seinem Service Edge DNS gemeldet. Dieser Dienst sorgt unter anderem dafür, dass Websites angesteuert werden können und vor Überlastungs-Attacken, sogenannten DDoS-Angriffen, geschützt werden.

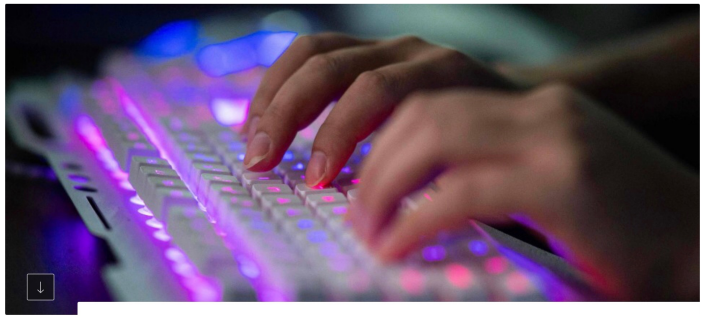
---

faz.net

Unternehmen Teilen Merken

Hacker erbeuten Daten und wollten Versicherung erpressen

AKTUALISIERT AM 22.07.2021 - 10:50



Als die hessische Versicherung den Angriff bemerkte, kappte sie die Verbindung ins Netz. Doch die Angreifer hatten bereits personenbezogene Daten gestohlen. Ihren Forderungen kam die Haftpflichtkasse dann nicht nach.

---

donaukurier.de

Nachrichten Lokales Polizei Sport Themen Freizeit Bilder & Videos Anzeigen Abo Junge Leser

BERLIN

erstellt am 02.08.2021 um 19:50 Uhr
aktualisiert am 02.08.2021 um 19:52 Uhr

Experte erwartet KI-Wettrüsten mit Hackern

Zuletzt sorgten Hacker-Angriffe mit Lösegeld-Trojanern auf große Unternehmen für Schlagzeilen. Einem Experten zufolge könnte der Kampf gegen Cyber-Attacken bald in eine andere Richtung weitergehen.

Mikko Hyppönen, Forschungschef der finnischen IT-Sicherheitsfirma F-Secure. Foto: Christoph Dernbach/dpa

Im Kampf gegen Cyberattacken kündigt sich nach Expertenmeinung ein Wettlauf mit Hackern bei künstlicher Intelligenz an.

Angreifer dürften bald dazu übergehen, ihre Schadsoftware automatisch von Algorithmen verändern zu lassen, damit sie nicht von Antivirenprogrammen erkannt wird, sagte der Forschungsschef der IT-Sicherheitsfirma F-Secure, Mikko Hyppönen, der Deutschen Presse-Agentur.

Hackerangriff-Simulation

Das machen wir

protekto
Für den Menschen

- Durchführung von simulierten Cyber-Attacken
- 400+ Angriffsszenarien in 65 Angriffskategorien
- Identifikation der Schwachstellen in der gesamten Internet-Sicherheitsarchitektur
- Überprüfung notwendiger Sicherheits-Patches

- Einschätzung der Sicherheitsstandards durch unsere Experten
- Ausführlicher, schriftlicher Report für Ihre Dienstleister

- eine ausführliche Video-Online-Beratung zur Erläuterung

Mit dieser Simulation schaffen Sie sich die optimale Grundlage für das nächste Gespräch mit Ihrer Internetagentur oder Ihrer IT-Abteilung.

Hackerangriff-Simulation

Ablauf

protekto
Für den Menschen

1. Auftrag erteilen
2. Cyber-Check-Vollmacht erteilen (kurzes Telefonat mit Protekto IT-Sicherheitsexperte)
3. Hackerangriff simuliert durchführen (die Attacke wird nicht final vollzogen)
4. Protekto IT-Sicherheitsexperte erstellt einen ausführlichen Bericht mit Umsetzungsempfehlungen
5. In einer ausführlichen (Video-) Beratung beantworten wir Fragen

Hackerangriff-Simulation

Das Team

protekto
Für den Menschen

Sprechstunde Datenschutz/IT-Sicherheit
Denise Loos

IT-Sicherheits-Experten
Alexander Riegert
Hendrik Gaffo

Datenschutz-Experten
André Wiederhold
Dirk Panitz
Kent Schwirz
Uwe Bücklein

Hackerangriff-Simulation
DSGVO-Check Cookies + Tracking

Die Pakete

protekto
Für den Menschen

Internet-Check „Hacker-Angriff-Simulation“

Der Internet-Check „Hacker-Angriff-Simulation“ kostet pro zu prüfender Internet-URL **398,00 €**

Internet-Check „Cookies + Tracking im Datenschutz“

Der Internet-Check „Cookies + Tracking im Datenschutz“
kostet pro zu prüfender Internet-URL **398,00 €**

20% sparen mit dem **Internet-Check-Kombi-Paket**
„Hacker-Angriff-Simulation“ plus „Cookies + Tracking im Datenschutz“

Im Auftrag zusammen kosten beide Internet-Checks „Hacker-Angriff-Simulation“ und „Cookies + Tracking im Datenschutz“ zusammen pro zu prüfender Internet-URL **nur 636,00 €**
Sie sparen 20% (160,00 €)

Hackerangriff-Simulation

Unterlagen

protekto
Für den Menschen

Information

protekto
Für den Menschen

Wie sicher sind Ihre Internetseiten gegen Hackerangriffe?

Mit einem simulierten Hackerangriff mit mehr als 400 verschiedenen technischen Angriffsszenarien können Sie Ihre Webseiten durch die Protekto auf Sicherheitsrisiken überprüfen lassen. Erkennen Sie dadurch Schwachstellen und minimieren Sie Angriffsflächen.

Einführung in die Hackerangriff-Simulation

In der heutigen Zeit ist die Webseite eines Unternehmens oftmals der erste Angriffspunkt für Cyberkriminelle - insbesondere, wenn die Angreifer wissen, dass potenziell wertvolle Daten zu holen sind. Daher ist es wichtig, frühestmöglich über die zugrundeliegenden Sicherheitsrisiken, die einen solchen Vorfall ermöglichen, informiert zu sein. Zugegebenermaßen ist das Thema Cyber-Security komplex und zeitaufwändig. Das Ziel der Protekto ist es, die Umsetzung für Kundinnen und Kunden so einfach wie möglich zu machen.

Unsere Hackerangriff-Simulation führt einen aktiven Penetrationstest durch. Um diesen durchführen zu können, benötigen wir die Einwilligung des Webseitenbetreibers. Bei der Durchführung stimmen wir uns eng mit dem Kunden ab.

Angriffsbeispiele

Wir nutzen die OWASP Top Ten als wichtigste Grundlage der Überprüfung von Sicherheitsmerkmalen von Webseiten. Zum aktuellen Zeitpunkt haben wir **65 Angriffskategorien** mit über **400 Angriffsszenarien** zusammengestellt, die bei einer Hackerangriff-Simulation zum Einsatz kommen.
Nachfolgend tauchen wir beispielhaft in zwei Angriffskategorien ein, um Ihnen eine Vorstellung darüber zu geben, wie unsere Hackerangriff-Simulation die Fehleranfälligkeit von Webseiten überprüft.

Beispiel 1: (No)SQL Injections

Aufgrund des Bedarfs an dynamischen Inhalten heutiger Webanwendungen sind die meisten Betreiber auf ein Datenbank-Backend angewiesen. Dort werden Daten gespeichert, die von der Webanwendung (oder anderen Programmen) abgerufen und verarbeitet werden können. Webanwendungen rufen Daten aus der Datenbank ab, indem sie SQL-Abfragen (z.B. für MySQL, MSSQL, PostgreSQL und Oracle) oder NoSQL-Abfragen (z.B. für MongoDB) verwenden.

Was ist eine (No)SQL Injection?

Eine (No)SQL Injection tritt auf, wenn ein Außenstehender von ihm stammende Werte innerhalb einer (No)SQL-Abfrage verwenden kann, ohne dass vorher eine Validierung dieser Werte durchgeführt wird. Dadurch kann er beliebigen (No)SQL-Code ausführen, um beispielsweise Datenbankabfragen vorzunehmen und Daten einzusehen.

Leistung

Spezial-Angebot »Datenschutz/IT-Sicherheit«
Internet-Check „Hacker-Angriff-Simulation"

protekto
Für den Menschen

Ist Ihre Website gegen Hacker-Angriffe geschützt?

Prüfen Sie die Sicherheit Ihrer Internetseite durch eine simulierte Cyber-Attacke

Jeden Tag wird in den Medien von Cyber-Attacken, von gekaperten Internetseiten, von nicht erreichbaren Webseiten und von gestohlen Passwörtern und vielem anderen berichtet. Die aktuellen Beispiele zeigen wieder einmal, mit welchen ausgeklügelten Methoden Cyber-Kriminelle heutzutage vorgehen. Erfolgreiche Angriffe verursachen enorme Schäden – nicht nur finanziell, sondern sie gefährden auch die Reputation des Unternehmens. **Überprüfen Sie deshalb die Sicherheit Ihrer Internetseite mit einem realistischen, jedoch simulierten Hacker-Angriff.**

So decken Sie Sicherheitslücken auf

Wir überprüfen anhand einer simulierten Cyber-Attacke die Sicherheit Ihrer Internetseite. Schwachstellen in der gesamten Internet-Sicherheitsarchitektur werden identifiziert. So erfahren Sie nicht nur, wie effektiv Ihre Internetseite vor Hacker-Angriffen geschützt ist, sondern Sie erhalten darüber hinaus konkrete Sicherheitsempfehlungen zur Optimierung Ihrer Sicherheitseinstellungen von unseren Datensicherheits-Experten.

Zum Ablauf Ihrer individuellen Prüfung

Unsere Experten setzen für die simulierte Cyber-Attacke gezielt unterschiedliche technische Methoden ein. Nach dem „Angriff" erhalten Sie einen aussagekräftigen Testbericht, in dem ausführlich erklärt wird, wie die Schwachstellen durch Hacker ausgenutzt werden könnten. Mit dieser Simulation schaffen Sie sich die optimale Grundlage für das nächste Gespräch mit Ihrer Internetagentur oder Ihrer IT-Abteilung.

Der Internet-Check „Hacker-Angriff-Simulation" der Protekto beinhaltet folgende Maßnahmen für eine Internet-URL:

- Durchführung von simulierten Cyber-Attacken mit 400+ Angriffsszenarien
- Identifikation der Schwachstellen in der gesamten Internet-Sicherheitsarchitektur
- Überprüfung notwendiger Sicherheits-Patches
- Ausführlicher, schriftlicher Report für Ihre Dienstleister
- Einschätzung der Sicherheitsstandards durch unsere Experten
- eine ausführliche Video-Online-Beratung zur Erläuterung

Der Internet-Check „Hacker-Angriff-Simulation" kostet für eine Internet-URL EUR 398,00 netto zzgl. MwSt. **Mit dem Kombi-Paket „Hacker-Angriff-Simulation" plus „Cookies + Tracking im Datenschutz" können Sie jetzt 20% sparen!**

„So erfahren Sie, wie effektiv Ihre Website vor Hacker-Angriffen geschützt ist!"

www.protekto.de