01/22
ITS
NEWS

What the Hack ist Log4j?

LOG4J beschäftigt Systemadministrator:innen weltweit

Java, das ist doch eine Insel in Indonesien oder eine Kaffeesorte? Tatsächlich handelt es sich bei Java auch um eine Programmiersprache. Vermutlich wurde der Name gewählt, weil Programmier:innen gern und viel Kaffee konsumieren. Log4j ist die Abkürzung für „Logging für Java“. Ein kleines Programm, das helfen soll, Fehler in Software zu finden, die mit Java geschrieben wurde. Leider hatte dieses Hilfsprogramm selbst einen Fehler, der es ermöglicht, Java Programme wie zum Beispiel Webserver zu hacken und dadurch großen Schaden anzurichten. Weil diese Schwachstelle relativ einfach auszunutzen war, schrillten Ende Dezember letzten Jahres überall auf der Welt in den IT Abteilungen die Alarmglocken. Eine ganze Reihe an Systemen war betroffen, selbst bei großen Unternehmen wie Tesla, Apple, Google oder Amazon. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gab eine rote Warnmeldung der höchsten Gefährdungsstufe heraus.

Im ITS brachte die Nachricht, dass Log4j ein massives Sicherheitsproblem darstellt, große Unruhe in die Vorweihnachtszeit. Schnelles Handeln war gefragt. Teilweise noch am Wochenende unmittelbar nach Bekanntwerden der Schwachstelle, wurden zahlreiche Server von den verantwortlichen Systemadministratoren überprüft und versucht, das Sicherheitsloch sofort zu schließen. In einem zweiten Schritt wurden möglicherweise betroffene Systeme überprüft, ob vielleicht bereits ein Angriff erfolgreich war. Nicht zuletzt durch dieses rasche Handeln konnte ein größerer Schaden für die IT Infrastruktur der Universität Bayreuth zumindest nach bisherigen Erkenntnissen abgewendet werden.

Gefahr erkannt – Gefahr gebannt?

Nicht ganz, denn auch in den nächsten Wochen und Monaten ist für das verantwortliche IT Personal erhöhte Aufmerksamkeit gefordert. Die eigentlichen Angriffe kommen möglicherweise noch. Niemand kann mit Sicherheit sagen, ob diese Schwachstelle nicht schon länger von Hackern entdeckt und ausgenutzt wurde. Solche erfolgreichen Angreifer spionieren die gehackten Systeme zunächst aus, um Passwörter oder andere sensible Informationen zu erbeuten oder möglicherweise

eine Hintertür oder ein anderes Schadprogramm zu installieren. Diese Zugänge werden dann im Darknet verkauft und dienen als Grundlage für weitere Angriffe bei denen zum Beispiel alle Daten auf einem Computer verschlüsselt werden, um Lösegeld zu erpressen oder Daten auf dem Server auszuspionieren, um diese für wirtschaftliche Zwecke zu nutzen. Solche Ransomware genannten Erpressungsversuche oder das Abgreifen von Daten könnten auch Wochen oder Monate nach der Erstinfektion von betroffenen Servern aus durchgeführt werden.

Ist auch mein Computer von Log4j betroffen?

Überwiegend geht es bei der Log4j Sicherheitslücke um Serverprogramme. Auf normalen PCs sind solche Programme eigentlich nicht installiert oder laufen zumindest nicht als von außen erreichbarer Serverdienst. Indirekt könnten aber User:innen betroffen sein, die einfach nur Dienste einer Internetseite verwenden. Zum Beispiel, weil dort Passwörter gestohlen werden, mit denen die Angreifer dann Zugriff auf universitäre Nutzerkonten bekommen. Denkbar wäre außerdem, dass ein gekaperter Server dazu gebracht wird, Schadsoftware als Updates zu tarnen und diese so an arglose Anwender:innen zu verteilen.

Was können Endanwender:innen tun?

Vor allem die Vorsichtsmaßnahmen treffen, die immer gelten. E-Mails die dazu auffordern einen bestimmten Link anzuklicken oder einen Download auszuführen immer kritisch hinterfragen. Außerdem die auf dem Computer installierte Software auf dem aktuellsten Stand halten und für die verschiedenen Logins bei Diensten wie Ebay, Amazon oder anderen Internetplattformen jeweils ein unterschiedliches Passwort verwenden. Diese Passwörter sollten außerdem nicht identisch mit dem Passwort für die dienstlichen Zugänge sein. Dadurch sinkt die Gefahr, dass ein gehackter Account dazu führt, dass gleich mehrere Profile eines Anwenders betroffen sind. Wer sichergehen möchte, sollte jetzt seine Passwörter zeitnah ändern. Als sicher gilt dabei eine mindestens zwölfstellige Kombination aus Zahlen, Buchstaben mit Groß- und Kleinschreibung und Sonderzeichen. Als kleiner Tipp hilft ein Merksatz, bei dem der jeweils erste Buchstabe als Bestandteil des Passwortes dient z.B: „mein neues Passwort 2022 – wegen log 4 j“ = „mnP2022-wl4j“. Das ITS bietet auf dem Panopto Server übrigens auch ein Schulungsvideo zum Thema Passwortsicherheit, das im Rahmen der Informationssicherheitswoche im Sommersemester 2021 entstanden ist.

www.its.uni-bayreuth.de/passwortsicherheit

Änderungen an der Zoom Lizensierung

Die Uni hat entschieden, die Zoom Campus Lizensierung nicht über den März 2022 hinaus zu verlängern. Das hat für Studierende und Beschäftige zur Folge, dass sie Zoom künftig nicht mehr unbegrenzt nutzen können. Mit den weiterhin verfügbaren Zoom Accounts werden dann nur noch Meetings von maximal 40 Minuten Dauer möglich sein.

Weitergehende Informationen zur Lizenzumstellung von Zoom und zum Nachfolger als Videokonferenztool MS-Teams finden Sie in folgenden FAQ:

www.its.uni-bayreuth.de/faq-zoom-teams

Mit MS-Teams steht schon nämlich längst eine umfangreichere, flexible Alternative zur Verfügung. Weshalb es sich lohnt sich Microsoft (MS) Teams und seine Möglichkeiten einmal genauer anzuschauen.

Teams verknüpft alle Office Programme miteinander. Sie können Word, Excel oder PowerPoint Dokumente über Teams teilen, Inhalte gemeinsam erstellen und gleichzeitig bearbeiten und dabei in Echtzeit kommunizieren. Dabei ist es möglich, verschiedene Teams (Gruppen) anzulegen. Berechtigungen und Teilnehmer werden individuell verwaltet. Auch Personen außerhalb der Universität Bayreuth können an einem Projekt via Teams teilnehmen und Zugriff auf Daten erhalten.

Als Nachfolgeprodukt zum altbekannten Skype ermöglicht Teams Videokonferenzen und Kommunikation von Angesicht zu Angesicht, sowie virtuelle Veranstaltungen und Webinare mit bis zu 300 Teilnehmern. Ähnlich zu Zoom kann die Teilnahme an der Konferenz nur via Audio oder auch via Mobilgerät, Einwahlnummer und App erfolgen.

Mit dem Messenger ist es möglich, in einer Gruppe oder mit einem einzelnen Teammitglied zu chatten. Wechseln Sie spontan zu einem Anruf oder teilen Sie einen Bildschirm. Mit der Teams App, welche in den bekannten Appstores erhältlich ist, chatten Sie auch unterwegs von Ihrem Handy.

MS Teams ist für Angehörige der Uni Bayreuth kostenfrei.

Für Fragen stehen Ihnen die Kollegen gerne zur Verfügung unter:

teams@uni-bayreuth.de.

Gastbeitrag Green Campus

Nachhaltiges Arbeiten

In den letzten beiden Jahren hat sich der Arbeitsalltag für einen Teil unserer Gesellschaft grundlegend geändert, da viele Menschen nun ganz oder teilweise im Homeoffice arbeiten. In den meisten Fällen spart dies im Vergleich zum täglichen Pendeln zum Arbeitsplatz CO2-Emissionen ein. Doch auch beim digitalen Arbeiten fallen Emissionen an. Diese können jedoch auf einfache Art und Weise reduziert werden. Im Nachfolgenden zeigen wir umsetzbare Tipps, mit denen wir unser digitales Arbeiten im Handumdrehen etwas nachhaltiger gestalten können.

Private E-Mail Accounts bewusst verwalten

„Im Jahr 2025 werden die weltweiten Server-Zentren für ein Fünftel des globalen Stromverbrauchs verantwortlich sein."
Quelle: Data Economy

Verwaltet man seine Email-Postfächer und löscht Mails, die man nie wieder brauchen wird, hilft das nicht nur der Übersicht, sondern trägt auch zu einem reduzierten Stromverbrauch bei. Das liegt hauptsächlich daran, dass auch nicht mehr benötigte Mails nach wie vor auf Servern liegen und somit für stetigen Energieverbrauch verantwortlich sind. Meldet man sich von unnötigen Newslettern ab, schaltet automatische Mail-Benachrichtigungen (z.B. von Social Media) aus und aktiviert im Spam-Ordner eine Funktion, die E-Mails nach kurzer Zeit automatisch löscht, hat man stets ein aufgeräumtes Postfach.

Externe Speichermedien der Cloud bevorzugen

Auch die Server von Cloud-basierten Speichern verbrauchen einiges an Energie. Wer für private Fotos und Videos externe Speichermedien wie Festplatten nutzt, um diese zu speichern, kann gegenüber der Cloud einen konstanten Energieverbrauch der Server einsparen. Somit wird bei Nicht-Verwendung der Daten auch keine Energie benötigt. Diesbezüglich ist es besonders hilfreich, wenn Daten bereits im Vorfeld bewusst verwaltet werden. Dabei hilft beispielsweise:

- Automatisches Speichern aller empfangenen Fotos ausschalten (Fotos bewusst speichern).
- Automatische Synchronisation mit der Cloud abstellen (Vermeidung von unnötigen Duplikaten)

Digitale Konferenzen

Auch wenn digitale Zusammenkünfte einiges an CO2-Emissionen gegenüber Präsenz-Meetings einsparen können, so sind sie lange nicht CO2-neutral. Gerade die Videoübertragung verbraucht einen erheblichen Anteil. Greenspector berechnet einen etwa 3 mal so hohen CO2-Ausstoß der beliebtesten Videokonferenz-Tools, wenn der Nutzer zum Audio auch noch das Video hinzuschaltet. Natürlich ist es schöner, sich bei einem Meeting zu sehen, da dies zusätzlich auch den Gesprächsfluss fördert. Daher empfiehlt es sich, die digitalen Konferenzen gut zu strukturieren. Je kürzer ein virtuelles Treffen gestaltet ist, desto weniger Daten fließen und dementsprechend weniger CO2-Emissionen fallen an.

Suchmaschinen

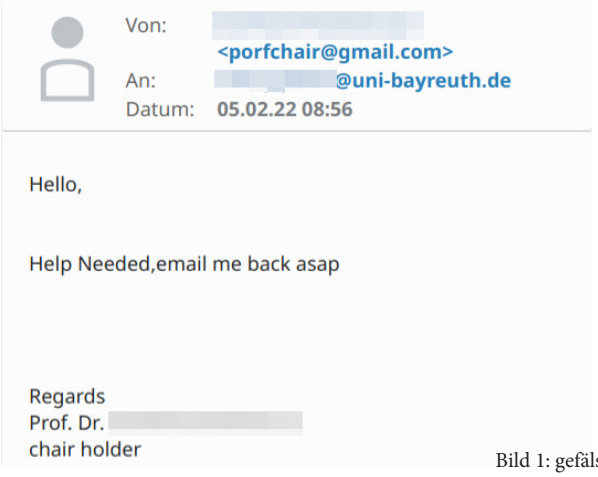
Ökologisch und sozial verträgliche(re) Alternativen gibt es nicht nur beim Strom, sondern auch bei Suchmaschinen. Nachfolgend stellen wir Euch zwei solcher Alternativen vor.

Die Suchmaschine Gexsi funktioniert wie ein Sozialunternehmen. Dabei generieren die Suchanfragen Einnahmen. Mit diesem Geld werden Projekte, die die 17 Sustainable Development Goals adressieren, unterstützt. Die Sustainable Development Goals (SDGs) der Vereinten Nationen sollen eine nachhaltige Entwicklung auf ökonomischer, ökologischer und sozialer Ebene sichern. Eine Auswahl der verschiedenen, unterstützten Projekte sind auf der Webseite von Gexsi aufgelistet. Bei Anklicken der Projekte, erhält man eine kurze Projektbeschreibung und kann entweder nachlesen, warum das Projekt ausgewählt wurde und/oder welche SDGs es adressiert.

Bei der Suchmaschine Ecosia wird durch 45 Suchanfragen eine Baumpflanzung finanziert. Mit den generierten Einnahmen, werden mehr als 20 Baumpflanzprojekte in 15 Ländern unterstützt (in Südamerika, Afrika und Asien). Die Baumpflanzungen erfolgen vor Ort mit der Unterstützung von lokalen Bauern und Bäuerinnen. Somit wird nicht nur die Biodiversität und Artenvielfalt gefördert, sondern den Menschen vor Ort werden ebenfalls Bewirtschaftungsalternativen angeboten. Der benötigte Strom zum Betreiben der Suchmaschine wird laut eigenen Angaben von Ecosia nachhaltig – teils aus eigenen Photovoltaikanlagen – bezogen.

Vorsicht: Teure Emails im Umlauf

Betrüger lassen sich immer neue Maschen einfallen. Aktuell sind Emails im Umlauf, in denen sich Kriminelle als Vorgesetzte ausgeben. Unter einem Vorwand werden Sie aufgefordert, Gutscheinkarten zu besorgen: STOPP! An dieser Stelle sollten Sie hellhörig werden.


Von: <porfchair@gmail.com>
An: @uni-bayreuth.de
Datum: 05.02.22 08:56

Hello,

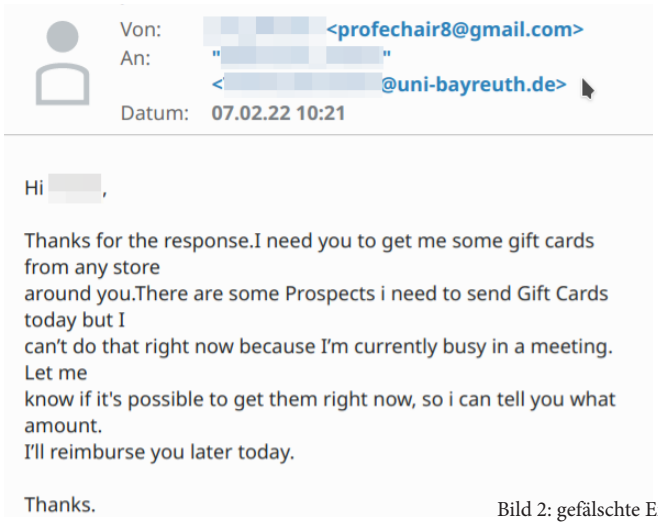
Help Needed,email me back asap

Regards
Prof. Dr.
chair holder

Bild 1: gefälschte Email

Diese Mails (Bild 1) enthalten erst einmal keine Schadelemente. Sie gibt lediglich vor, von Ihrem/Ihrer Vorgesetzte:n zu stammen. Die Absenderemailadresse „profchair@gmail.com“ gibt einen ersten Hinweis darauf, dass es sich um eine Fälschung handelt. Selbst wenn man darauf antwortet, weil man in Eile ist und den gefälschten Absender übersieht, ist noch nichts passiert. Meist erhalten Sie nun eine weitere gefälschte Email (Bild2), die vorgibt, Ihr/e Vorgesetze:r bräuchte Geschenkkarten bekannter Dienste wie Google oder Amazon.

Kritisch wird es, wenn Sie die Nummern der Geschenkkarten an die Angreifer schicken. Diese Codes werden sofort verwertet. Und der finanzielle Schaden bleibt.


Von: <profechair8@gmail.com>
An: "" <@uni-bayreuth.de>
Datum: 07.02.22 10:21

Hi ,

Thanks for the response.I need you to get me some gift cards from any store
around you.There are some Prospects i need to send Gift Cards today but I
can't do that right now because I'm currently busy in a meeting. Let me
know if it's possible to get them right now, so i can tell you what amount.
I'll reimburse you later today.

Thanks.

Bild 2: gefälschte Email

Wenn Sie also solche oder ähnliche Emails bekommen, beachten Sie bitte die folgenden Sicherheitsmaßnahmen:

- Prüfen Sie die Absenderemailadresse und vergleichen Sie diese mit der Ihnen bekannten Emailadresse. Persönliche Emailadressen werden an der Uni in der Regel in folgender Form vergeben: **vorname.nachname@** uni-bayreuth.de.
- Seien Sie besonders aufmerksam, wenn Sie Emails auf dem Handy oder Tablets abfragen.
- Fragen Sie bei dem vermeintlichen Absender auf einem anderen Weg z.B. per Telefon nach.
- Lassen Sie sich nicht unter Druck setzen, auch wenn Sie in Eile sind.
- Wenden Sie sich im Zweifel an die Informationssicherheit (its-security@uni-bayreuth.de).

HINWEIS:

Vorankündigung: Die IT-Sicherheitswoche findet vorraussichtlich in der Zeit vom 28. März bis zum 01. April 2022 statt. Genauere Informationen erfahren Sie in Kürze über unsere Homepage.

IMPRESSUM:

Herausgeber:
IT-Servicezentrum
Universität Bayreuth
Universitätsstraße 30
95447 Bayreuth

Leitender Redakteur: Oliver Gschwender
Autoren: Oliver Gschwender, Claudia Willer, Ralf Stöber, GreenCampus Jennifer Pflügler
Foto: Foto von Mati Mango von Pexels
Druck: Eigendruck

www.its.uni-bayreuth.de