VORFALL-LAGEBILD

Cyberangriff auf Webserver der Charité Berlin: Kontaktdaten abgeflossen

Stand 02.11.2026 14:56 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach allem, was bekannt ist, war der Webserver betroffen und die Versorgung nicht. Für die Betroffenen ist der Schaden trotzdem real, weil Name, Mail und Charité-Bezug perfekte Zutaten für Betrugsmails sind.

2. Ein Kontaktformular ist ein Eingang ins Haus: Was dort ankommt, sollte schnell weg vom Webserver und nach festen Fristen gelöscht werden.

3. Ob Klinik oder Industrieanlage, die Grundregel bleibt gleich: Öffentliche Systeme sauber vom Rest trennen (CC2 Defensible Architecture), schnell patchen nach Risiko (CC5) und einen geübten Ablauf für den Ernstfall haben (CC1).

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Unbekannte haben sich Zugriff auf einen Webserver der Charité verschafft und Daten erbeutet (Stellungnahme der Charité).	100 %	100 %	bestätigt
Betroffen ist laut Charité-Rundmail eine Datei mit Angaben zu Personen; laut Charité handelt es sich um Name und Organisationszugehörigkeit.	100 %	85 %	präzisiert
Der Zugangsweg wurde laut Charité-Sprecher zügig identifiziert und geschlossen, die Ursache wurde analysiert und die Schutzmaßnahmen wurden verstärkt.	100 %	100 %	bestätigt
Laut Charité hat der Angriff nichts mit der weltweiten PHP-Sicherheitslücke aus der Vorwoche zu tun.	100 %	100 %	bestätigt
Der Einstieg lief über eine Schwachstelle oder Fehlkonfiguration in der Web-Anwendung selbst (CMS, Erweiterung, Formular-Komponente), nicht über das interne Kliniknetz.	60 %	60 %	offen
Es gibt doch einen Zusammenhang mit php2shell (laut Charité ausgeschlossen).	15 %	12 %	offen
Abgeflossen sind personenbezogene Kontaktdaten von Mitarbeitenden und Studierenden sowie von externen Personen, die über das Kontaktformular Kontakt aufgenommen hatten, etwa für Terminanfragen.	100 %	100 %	bestätigt
Die Krankenversorgung war laut Charité nicht beeinträchtigt; sensible Gesundheitsdaten von Patienten sind nach aktuellem Stand nicht betroffen.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Wie viele Daten abgeflossen sind, ist noch unbekannt.	100 %	5 %	teilweise widerlegt: Sprecher nennt Schätzungen (Ärzteblatt), offizielle Zahl fehlt
Bisher ist nicht bekannt, dass die Daten veröffentlicht oder missbraucht wurden.	100 %	100 %	bestätigt
Die Website war am Dienstag zeitweise nicht erreichbar, weil der betroffene Server isoliert und vom Netz genommen wurde.	100 %	100 %	bestätigt
Die Betroffenen bekommen gezielte Phishing-Mails, die sich als Charité ausgeben.	55 %	50 %	offen
Klinische Systeme wurden mitkompromittiert.	8 %	6 %	offen
Der betroffene Server wurde isoliert, die Website war am Dienstag nur kurz nicht erreichbar.	100 %	100 %	bestätigt
Die Charité hat ein externes IT-Unternehmen beauftragt und Strafanzeige erstattet.	100 %	50 %	präzisiert: Strafanzeige belegt (ComputerBase, Ärzteblatt), externes IT-Unternehmen für die Charité nicht sicher belegt
Der sichtbare Betrieb ist weitgehend wiederhergestellt, die forensische Aufarbeitung dauert noch Wochen.	70 %	70 %	offen
Die Krankenversorgung war laut Charité in keiner Weise beeinträchtigt.	100 %	100 %	bestätigt
Medizintechnik, Gebäudetechnik oder andere klinische Betriebstechnik sind nicht betroffen.	88 %	88 %	offen
Wegen der PHP-Lücke php2shell (CVE-2026-109618/-109619) haben neben der Charité (21.10.) auch die Unikliniken Köln, Düsseldorf, Freiburg, Heidelberg und Mannheim ihre Websites vorsorglich vom Netz genommen.	100 %	90 %	präzisiert
Der Forscher Silas Cutler schätzt laut Tenable grob über 1,3 Millionen aus dem Internet erreichbare, möglicherweise verwundbare PHP-Hosts weltweit; andere Zählungen kommen auf deutlich andere Werte.	100 %	100 %	bestätigt
Die Universität Leipzig hat nach einem Angriff am 28.10. vorsorglich alle Server mit Internetanbindung vom Netz genommen, Website und E-Mail fielen aus.	100 %	100 %	bestätigt
Fast jedes Krankenhaus und jede Hochschule betreibt Websites mit Kontakt- oder Terminformularen, die aus dem Internet erreichbar sind.	85 %	85 %	offen

Frühere Aussage	vorher	jetzt	Status
Die US-Behörde CISA hat php2shell am 26.10.2026 in ihren Katalog aktiv ausgenutzter Schwachstellen aufgenommen.	100 %	100 %	bestätigt
Das BSI hat die PHP-Lücken mit Warnstufe 3 (orange) bewertet.	100 %	100 %	bestätigt
Kliniken in DACH werden in den kommenden Monaten weitere Datenabflüsse über öffentlich erreichbare Webdienste melden.	75 %	75 %	offen

Neu seit dem letzten Stand

• Laut Charité-Sprecher gegenüber dem Ärzteblatt sind rund 46.000 Mitarbeitende und Studierende, rund 1.500 Newsletter-Empfänger und rund 90.000 Formularnutzer betroffen; das Ärzteblatt titelt „knapp 140.000“, die Charité-Erklärung nennt keine Zahl.

• Datenarten präzisiert: Vor- und Nachname, E-Mail-Adresse, gegebenenfalls Organisation; bei Beschäftigten laut MAZ auch Benutzernamen; Freitext-Nutzer werden einzeln informiert.

• Ausfalltag präzisiert: 27.10.2026; erste vorsorgliche Abschaltung wegen PHP am 21.10.

• Parallele Vorfälle: Universität Kopenhagen (rund 525.000 Betroffene), Universität Leipzig, Humboldt-Universität Berlin (IT-Sicherheitsvorfall laut Ärzteblatt).

Wissensstand



■ Wissen 44 % ■ Wahrscheinlich 20 % ■ Nicht bekannt 36 %

Die Kernfakten stammen von der Charité selbst (Erklärung auf charite.de vom 30.10., Rundmail, Sprecher gegenüber dem Ärzteblatt). Die Betroffenenzahlen sind Schätzungen eines Sprechers aus einer einzigen Quelle. Zu Zugangsweg, Zeitpunkt und Täter gibt es öffentlich nichts.

1. Was ist passiert, und warum?

WISSEN

• Unbekannte haben sich Zugang zum Webserver der Charité verschafft, auf dem auch die öffentliche Website liegt, und dort personenbezogene Kontaktdaten erbeutet. (100 %) [https://www.charite.de/die_charite/themen/cyberangriff_auf_charite_webserver/]

• Laut Charité-Sprecher ist der Zugangsweg „zügig identifiziert und geschlossen“ worden, die Ursache wurde analysiert, die Schutzmaßnahmen wurden verstärkt. (100 %) [https://www.tagesspiegel.de/berlin/dpa-kriminalitat-cyberangriff-auf-charite-kontaktdaten-erbeutet-16219255.html]

• Laut Charité hat der Angriff nichts mit der weltweiten PHP-Lücke zu tun, wegen der sie ihre Website am 21.10. vorsorglich vom Netz genommen hatte. (100 %) [https://www.kma-online.de/aktuelles/it-digital-health/detail/charite-berlin-cyberangriff-auf-webserver-daten-abgegriffen-56426]

• In der Rundmail an Betroffene heißt es: „Dabei war leider auch eine Datei betroffen, die Angaben zu Ihrer Person enthalten“. (100 %) [https://www.tagesspiegel.de/wissen/personliche-daten-sind-abgeflossen-berliner-charite-von-hackerangriff-betroffen-16218667.html]

NICHT BEKANNT

• Über welchen Weg die Angreifer eingedrungen sind (die Charité nennt ihn nicht)

• Wann der Angriff stattfand und wann er entdeckt wurde

• Wer dahintersteckt und ob es eine Erpressung gibt

• Welche Software auf dem Webserver lief

WAHRSCHEINLICH (Einschätzung)

• Der Einstieg lief über eine Schwachstelle oder Fehlkonfiguration in der Web-Anwendung selbst (CMS, Erweiterung, Formular-Komponente), nicht über das interne Kliniknetz. (60 %) – Betroffen ist laut Charité der Webserver, auf dem auch die Website liegt, und die Daten stammen aus

Formularen und Verteilern. Das ist ein typisches Muster für Angriffe auf Web-Anwendungen. Einen Beleg für den Weg gibt es nicht.

• Es gibt doch einen Zusammenhang mit php2shell. (12 %) – Die Charité schließt das nach eigener Ursachenanalyse aus, unabhängig prüfen lässt sich das nicht. Einziger Anhaltspunkt ist der zeitliche Ablauf.

• Es waren finanziell motivierte Täter, die Daten verkaufen oder für Phishing nutzen wollen. (45 %) – Das ist bei Datendiebstahl ohne Verschlüsselung häufig, aber es gibt weder ein Bekennerschreiben noch einen Leak-Eintrag.

2. Was ist die Auswirkung?

WISSEN

• Ein Charité-Sprecher geht laut Ärzteblatt davon aus, dass circa 46.000 Mitarbeitende und Studierende, circa 1.500 Empfänger des Presse- und Newsletterverteilers und 90.000 Nutzer des Kontaktformulars betroffen sind; das Ärzteblatt titelt „knapp 140.000 Kontaktdaten“. (100 %) [https://www.aerzteblatt.de/news/charite-knapp-140000-kontaktdaten-bei-cyberangriff-abgeflossen-2c5a0f50-38aa-43f2-8fd9-1163f6deef74]

• In ihrer eigenen Erklärung vom 30.10.2026 nennt die Charité keine Zahl der Betroffenen. (100 %) [https://www.charite.de/die_charite/themen/cyberangriff_auf_charite_webserver/]

• Abgeflossen sind Vor- und Nachnamen, E-Mail-Adressen und gegebenenfalls Organisationszugehörigkeiten; Gesundheitsdaten nach Art. 9 DSGVO sind laut Charité „ausdrücklich nicht betroffen“. (100 %) [https://www.aerzteblatt.de/news/charite-knapp-140000-kontaktdaten-bei-cyberangriff-abgeflossen-2c5a0f50-38aa-43f2-8fd9-1163f6deef74]

• Bei Beschäftigten sollen laut MAZ-Informationen auch Benutzernamen betroffen sein. (100 %) [https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

• Wer das Freitextfeld des Terminformulars genutzt hat, wird von der Charité einzeln informiert; das Ärzteblatt hält es für naheliegend, dass dort Angaben zum Anliegen stehen können. (100 %) [https://www.aerzteblatt.de/news/charite-knapp-140000-kontaktdaten-bei-cyberangriff-abgeflossen-2c5a0f50-38aa-43f2-8fd9-1163f6deef74]

• Die Krankenversorgung war laut Charité nicht beeinträchtigt; Hinweise auf Veröffentlichung oder Missbrauch der Daten gibt es laut Charité bisher nicht. (100 %) [https://www.aerzteblatt.de/news/charite-knapp-140000-kontaktdaten-bei-cyberangriff-abgeflossen-2c5a0f50-38aa-43f2-8fd9-1163f6deef74]

• Die Website war am 27.10.2026 (Dienstag) zeitweise nicht erreichbar, weil die betroffenen Server isoliert und vom Netz genommen wurden. (100 %) [https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

NICHT BEKANNT

• Die genaue Zahl der Betroffenen: Die Charité hat keine offizielle Gesamtzahl veröffentlicht, die Sprecher-Zahlen sind Schätzungen

• Aus welchem Zeitraum die Formulardaten stammen

• Ob Freitexte mit Gesundheitsbezug tatsächlich abgeflossen sind

• Ob die Benutzernamen für weitere Angriffe genutzt werden können

• Ob die Daten schon verkauft oder veröffentlicht wurden

WAHRSCHEINLICH (Einschätzung)

• Betroffene bekommen in den nächsten Wochen gezielte Phishing-Mails, die sich als Charité ausgeben. (50 %) – Name, E-Mail und Bezug zur Charité sind genau das Material für glaubwürdiges Phishing, und die Charité warnt selbst davor. Konkrete Fälle sind bisher nicht berichtet.

• Klinische Systeme wurden mitkompromittiert. (6 %) – Die Charité nennt nur den Webserver und keine Einschränkung der Versorgung; es gibt keinen Hinweis auf eine Ausbreitung.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Die betroffenen Server wurden isoliert und vom Netz genommen, die Website war am 27.10. nur zeitweise nicht erreichbar. (100 %)
[https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

• Die Charité hat Strafanzeige erstattet. (100 %)
[https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

NICHT BEKANNT
• Ob die forensische Untersuchung abgeschlossen ist

• Ob der Webserver neu aufgesetzt oder nur bereinigt wurde

• Ob die Charité einen externen IT-Dienstleister für die Forensik beauftragt hat (für die Charité nicht sicher belegt)

WAHRSCHEINLICH (Einschätzung)
• Der sichtbare Betrieb ist weitgehend wiederhergestellt, die forensische Aufarbeitung dauert noch Wochen. (70 %) – Die Ausfallzeit war laut Berichten kurz, Forensik und Benachrichtigung von knapp 140.000 Personen brauchen nach Erfahrung mit ähnlichen Fällen deutlich länger.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN
• Die Krankenversorgung war laut Charité weder beeinträchtigt noch ist sie aktuell eingeschränkt. (100 %) [https://www.kma-online.de/aktuelles/it-digital-health/detail/charite-berlin-cyberangriff-auf-webserver-daten-abgegriffen-56426]

NICHT BEKANNT
• Ob die Charité Medizintechnik oder Gebäudetechnik eigens geprüft hat (dazu gibt es keine Aussage)

WAHRSCHEINLICH (Einschätzung)
• Medizintechnik, Gebäudetechnik oder andere klinische Betriebstechnik sind nicht betroffen. (88 %) – Betroffen ist nach allen Angaben ein öffentlich erreichbarer Webserver; eine Verbindung zur Betriebstechnik ist nicht berichtet, und die Versorgung lief normal.

5. Wie viele solcher Ziele gibt es?

WISSEN
• Wegen der PHP-Lücke hatten neben der Charité auch die Unikliniken Köln, Düsseldorf, Freiburg, Heidelberg und Mannheim ihre Websites vorübergehend abgeschaltet. (100 %) [https://www.kma-online.de/aktuelles/it-digital-health/detail/charite-berlin-cyberangriff-auf-webserver-daten-abgegriffen-56426]

• Der Forscher Silas Cutler schätzt laut Tenable grob über 1,3 Millionen aus dem Internet erreichbare, möglicherweise verwundbare Hosts; eine Shodan-Suche zählt über 1,9 Millionen Hosts mit PHP insgesamt. (100 %) [https://www.tenable.com/blog/php2shell-cve-2026-109618-cve-2026-109619-frequently-asked-questions-about-critical-php-remote]

• Die Universität Leipzig hat nach einem Angriff am 28.10. alle Server mit Internetanbindung vom Netz genommen; Website, E-Mail und Studienportale fielen aus. (100 %)
[https://newstime.joyn.de/themen/wirtschaft/hackerangriff-uni-leipzig-alle-server-lahmgelegt-208194]

• Die Universität Kopenhagen meldete einen Datenabfluss mit rund 525.000 Betroffenen über eine Testumgebung, entdeckt am 20.10. (100 %)
[https://www.infosecurity-magazine.com/news/copenhagen-university-data-breach/]

NICHT BEKANNT
• Wie viele deutsche Kliniken Formulardaten dauerhaft auf dem Webserver speichern

• Ob es zwischen den Vorfällen an Charité, Leipzig, Humboldt-Universität und Kopenhagen einen Zusammenhang gibt

WAHRSCHEINLICH (Einschätzung)
• Fast jedes Krankenhaus und jede Hochschule betreibt aus dem Internet erreichbare Websites mit Kontakt- oder Terminformularen. (85 %) – Das ist heute Standard für Patientenservice und Bewerbungen; eine Zählung dazu gibt es nicht.

6. Kann das wieder passieren?

WISSEN

• Die US-Behörde CISA hat die beiden php2shell-Lücken am 26.10.2026 in ihren Katalog aktiv ausgenutzter Schwachstellen aufgenommen. (100 %)
[https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog]

• Das BSI bewertet die PHP-Lücken mit der Warnstufe 3 / Orange (Bericht vom 21.10.2026). (100 %) [https://zdfheute.de/politik/sicherheitsluecke-php-webseiten-onlinedienste-cybersicherheit-bsi-100.html]

NICHT BEKANNT

• Ob der konkrete Zugangsweg bei der Charité auch bei anderen Kliniken besteht, solange er nicht bekannt ist

WAHRSCHEINLICH (Einschätzung)

• Kliniken in DACH werden in den kommenden Monaten weitere Datenabflüsse über öffentlich erreichbare Webdienste melden. (75 %) – Eine aktiv ausgenutzte PHP-Lücke, viele ungepatchte Altversionen und mehrere Hochschulvorfälle binnen einer Woche sprechen dafür.

Lage

Unbekannte sind in den Webserver der Charité eingedrungen, auf dem auch die öffentliche Website liegt, und haben Kontaktdaten erbeutet: Vor- und Nachnamen, E-Mail-Adressen und teils Organisationszugehörigkeiten. Ein Charité-Sprecher geht laut Ärzteblatt von circa 46.000 Mitarbeitende und Studierende, circa 1.500 Empfänger des Presse- und Newsletterverteilers und 90.000 Nutzer des Kontaktformulars aus (Überschrift: „knapp 140.000“); eine offizielle Gesamtzahl hat die Charité nicht veröffentlicht. Laut Charité waren Krankenversorgung und Gesundheitsdaten nicht betroffen, und der Angriff hängt nicht mit der PHP-Lücke php2shell zusammen. Zugangsweg, Zeitpunkt und Täter hat die Charité nicht genannt.

Angriff	Eindringen in den Webserver der Charité (Hosting der öffentlichen Website) und Diebstahl einer Datei mit Kontaktdaten; laut Sprecher geschätzt knapp 140.000 Personen
Wann / Status	Angriffszeitpunkt nicht veröffentlicht; Server am 27.10.2026 isoliert, Bekanntgabe am 30.10.2026 · eingedämmt
Täter	unbekannt – unbekannt
Betreiber / Branche	Charité, Universitätsmedizin Berlin · Gesundheitswesen, Universitätsklinikum (KRITIS-Sektor Gesundheit)
Anlage / Alter	Öffentlich erreichbarer Webserver mit Website und Kontaktformular (IT, keine OT) ·
Region	Berlin
Auswirkungen	Laut Charité keine Auswirkung auf die Krankenversorgung und keine Gesundheitsdaten nach Art. 9 DSGVO betroffen. Für die Betroffenen steigt das Risiko für gezieltes Phishing und Betrugsanrufe (Einschätzung). Die Charité rät zu Wachsamkeit bei Kontaktaufnahmen durch Unbekannte und betont, sie werde grundsätzlich nicht telefonisch nach Passwörtern fragen (Ärzteblatt).
Behörden	Die Charité steht laut eigener Aussage in engem Austausch mit den „zuständigen Aufsichts- und Ermittlungsbehörden“ und hat Strafanzeige erstattet (kma, Ärzteblatt). Welche Behörden konkret (etwa Berliner Datenschutzbeauftragte, LKA, BSI), ist nicht veröffentlicht.

Regulatorik	DSGVO: Meldung einer Datenschutzverletzung an die Aufsichtsbehörde binnen 72 Stunden (Art. 33) und Benachrichtigung der Betroffenen (Art. 34); die Charité informiert Betroffene einzeln. NIS2: Das neue BSIG gilt seit 6.12.2025 und sieht gestufte Meldungen an das BSI vor (24 Stunden Frühwarnung, 72 Stunden Bericht, ein Monat Abschlussbericht, https://www.ebnerstolz.de/de/unser-angebot/leistungen/rechtsberatung/it-recht-und-datenschutz/nis-2-deutschland-neues-bsig-in-kraft-104215.html). Ob die Charité den Vorfall als erheblichen Sicherheitsvorfall nach BSIG gemeldet hat, ist nicht bekannt. Dass sie als großes Uniklinikum unter die KRITIS- bzw. NIS2-Pflichten fällt, ist naheliegend, aber von mir nicht am Gesetzestext geprüft (vermutet).

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Schwachstelle in der Web-Anwendung (CMS, Erweiterung, Formular-Komponente), unabhängig von php2shell (hoch): Daten lagen auf dem Webserver selbst, nur dieser Server ist betroffen; Web-Anwendungen mit Formularen sind ein häufiger Einstieg bei Kliniken und Hochschulen.

• Gestohlene oder schwache Zugangsdaten für den Verwaltungszugang des Webservers oder des CMS (z. B. aus Phishing oder Credential Stuffing) (mittel): Typischer Weg bei Webservern mit vielen Redakteuren; die erwähnten Benutzernamen von Beschäftigten passen dazu, belegen es aber nicht.

• Kompromittierung über einen Dienstleister oder eine eingebundene Fremdkomponente (Supply Chain) (gering): Kommt im Klinikumfeld vor (Ärzteblatt erwähnt einen früheren Dienstleister-Vorfall bei Unikliniken), die Charité nennt aber keinen Dienstleister als Ursache.

• php2shell (CVE-2026-109618/-109619) (gering): Zeitlich naheliegend, von der Charité aber ausdrücklich ausgeschlossen.

Zeitleiste

21.10.2026 Das BSI warnt vor der PHP-Lücke, die Charité nimmt ihre Website vorsorglich offline – berichtet [https://www.kma-online.de/aktuelles/it-digital-health/detail/charite-berlin-cyberangriff-auf-webserver-daten-abgegriffen-56426]

26.10.2026 CISA nimmt php2shell in den Katalog aktiv ausgenutzter Schwachstellen auf – bestätigt [https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog]

27.10.2026 (Dienstag) Betroffene Charité-Server werden isoliert, die Website ist zeitweise nicht erreichbar – berichtet [https://www.computerbase.de/news/wirtschaft/kritische-infrastruktur-hacker-stehlen-daten-der-berliner-charite.100094/]

28.10.2026 Angriff auf die Universität Leipzig, alle Server mit Internetanbindung vom Netz – berichtet [https://newstime.joyn.de/themen/wirtschaft/hackerangriff-uni-leipzig-alle-server-lahmgelegt-208194]

30.10.2026 Die Charité bestätigt den Angriff in einer Erklärung und informiert Betroffene per Rundmail; eine Zahl nennt die Erklärung nicht – bestätigt [https://www.charite.de/die_charite/themen/cyberangriff_auf_charite_webserver/]

30.10.2026 Ein Charité-Sprecher nennt dem Ärzteblatt geschätzte Teilzahlen der Betroffenen (circa 46.000 Mitarbeitende und Studierende, circa 1.500 Empfänger des Presse- und Newsletterverteilers und 90.000 Nutzer des Kontaktformulars) – berichtet [https://www.aerzteblatt.de/news/charite-knapp-140000-kontaktdaten-bei-cyberangriff-abgeflossen-2c5a0f50-38aa-43f2-8fd9-1163f6deef74]

Vergleichsfälle

• Universität Kopenhagen, Datenabfluss über eine Testumgebung (rund 525.000 Betroffene) (2026): Auch Test- und Nebensysteme mit echten Daten sind ein Einstieg und gehören ins Asset-Inventar. [https://www.infosecurity-magazine.com/news/copenhagen-university-data-breach/]

• Universität Leipzig, alle internetnahen Server vom Netz (2026): Wer schnell isoliert, begrenzt den Schaden, braucht aber einen geübten Notfallplan für Mail und Website.
[https://newstime.joyn.de/themen/wirtschaft/hackerangriff-uni-leipzig-alle-server-lahmgelegt-208194]

Begriffe einfach erklärt

Webserver: Der Rechner, der eine Website ins Internet ausliefert und oft auch Formulareingaben speichert.

Phishing: Betrugsmails oder Anrufe, die sich als bekannte Absender ausgeben, um an Passwörter oder Geld zu kommen.

Patch: Ein Software-Update, das eine Sicherheitslücke schließt.

Segmentierung: Das Netz wird in getrennte Bereiche aufgeteilt, damit ein Einbruch an einer Stelle nicht überall hinführt.

OT: Betriebstechnik, also Technik, die Maschinen, Anlagen oder Gebäude steuert, im Unterschied zur Büro-IT.

Früherer Stand: Erstmeldung (30.10.2026 14:37)

Wissen 45 % · wahrscheinlich 21 % · nicht bekannt 34 %
Unbekannte sind in einen Webserver der Charité eingedrungen und haben Kontaktdaten von Beschäftigten, Studierenden und externen Personen abgegriffen, die das Kontaktformular der Website genutzt hatten. Laut Charité ist die Krankenversorgung nicht beeinträchtigt, nach aktuellem Stand sind keine Patientendaten betroffen, der Zugangsweg ist geschlossen und es wurde Strafanzeige erstattet. Die Charité selbst schließt einen Zusammenhang mit der kritischen PHP-Lücke php2shell aus, wegen der sie ihre Website am 21.10.2026 vorsorglich vom Netz genommen hatte; die Abschaltung am Dienstag, 27.10., gehört laut t-online und Tagesspiegel dagegen zum Angriff.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.