



Auf Erfolgskurs: Das „Team ohne Namen“ vom Berufskolleg Wirtschaft des Kreises Heinsberg in Geilenkirchen steht im Finale beim Netrace. FOTOS: MARC HECKERT

Das letzte Durchatmen

In der Hauptrunde des 17. Internetwettbewerbs von AZ und NetAachen haben sich 41 Teams für das Finale von Netrace qualifiziert. Und das beginnt am kommenden Dienstag.

VON MARC HECKERT

AACHEN/DÜREN/HEINSBERG Die Zeit zwischen der Hauptrunde und dem Finale ist beim Netrace die letzte Gelegenheit, noch einmal durchzuatmen, sich zu sortieren und die Strategie für die beiden Endrunden festzuklopfen. In den beiden Finalrunden werden die Ergebnisse aufeinander addiert, das heißt, Fehler in der ersten Finalrunde schlagen aufs Ergebnis durch. Nach der Hauptrunde dagegen wird der Punktstand aller



qualifizierten Teams dagegen noch einmal auf Null gesetzt. Alle Gruppen starten also mit gleichen Chancen. Es sind genau 41 Teams, die es ins Finale geschafft haben. Im Herbst waren 179 Gruppen von Schulen aus der Städteregion Aachen und den Kreisen Heinsberg und Düren an den Start gegangen. Davon hatten es 84 in die Hauptrunde geschafft.

Eines der Teams, die in der Hauptrunde am besten abgeschnitten haben, ist das „Team ohne Namen“ des Berufskollegs Wirtschaft des Kreises Heinsberg in Geilenkirchen. Die angehenden Gymnasiasten mit Schwerpunkt Betriebswirtschaftslehre aus der Klasse GYW 231 sind mit 47 von

50 Punkten an der Spitze des Tabellenfeldes. Nur vier Teams hatten die volle Punktzahl geschafft.

Da das „Team ohne Namen“ als komplette Klasse zu den großen Gruppen zählt, hatten die 23 Schülerinnen und Schüler den Luxus, dass sich viele Köpfe um die jeweils fünf Aufgabenblöcke kümmern konnten. „Wir haben uns in A, B, C, D und E aufgeteilt“, erklärt Schülerin Hannah. „Jede Gruppe hat eine Frage durchgearbeitet und dann den anderen geholfen.“ Die Ergebnisse wurden mit Hilfe der Online-Plattform Microsoft Teams gesammelt. Die Taktik der 16- bis 18-Jährigen ging auf. Gearbeitet wurde im WiFo-Unterricht, sprich: Wirtschaftsinformatik, wie ihre Lehrerin Beate Schreiber erklärt. Sie selbst macht schon seit vielen Jahren beim Netrace mit, ihre Schule war auch schon zweimal in den Top Ten vertreten. Die Lehrerin muss vom Netrace-Konzept nicht mehr überzeugt werden. „Ich finde die Idee total spannend“, sagt sie. „Es ist interessant zu beobachten, wie der Lernprozess während des Wettbewerbs verläuft und die Schüler immer selbständiger und kreativer werden.“

Vor allem das Arbeiten im Team sei eine ausgezeichnete Erfahrung für die Teilnehmer. Und nicht nur das: „Das Netrace hilft unfassbar, das Recherchieren zu lernen.“ Selbst wenn ein Team sich am

Anfang etwas schwer tue, entwickeln die Schüler oft regelrecht Biss. Da würden die Fragen auch dann noch weiterbeackert, wenn längst der Pausengong ertönt hat und die nächste Unterrichtsstunde schon begonnen hat. Beate Schreiber kann das gut nachvollziehen: „Ich kann da auch nicht aufhören, bis ich alles herausgefunden habe.“

Den Lernprozess bestätigen die Projektbetreuer vom Medienpädagogischen Institut Promedia Maassen aus Alsdorf den Teilnehmern ebenfalls. Typische Fehler wurden in der Hauptrunde nur noch selten gemacht. „Es wurden zwar beispielsweise auch wieder Wikis als Quellen eingereicht, aber insgesamt weniger“, sagt Hanna Höppler. „Aber auch in dieser Runde hat man wieder gesehen, dass an einigen Stellen nicht genau gelesen wurde“, erklärt ihre Kollegin Julia Vallet. In der ersten Teilfrage von Fragenkomplex 1 wurde etwa gefragt, an welchem Datum Ludwig XIV. – den richtigen König musste man vorher durch Recherchieren herausbekommen – als Kind zum König ernannt wurde. „Ein paar Teams haben hier das Datum der tatsächlichen Krönung angegeben, die aber erst im Erwachsenenalter stattfand“,

„Es ist interessant zu beobachten, wie der Lernprozess während des Wettbewerbs verläuft und die Schüler immer selbständiger und kreativer werden.“
Beate Schreiber, Lehrerin

bedauert die Projektbetreuerin. Genaues Lesen bleibt das A und O für Netrace-Punkte.

Bei der zweiten Teilfrage der zweiten Aufgabe wurde wiederum danach gefragt, nach welcher Verwandten des letzten Müllers eine Mühle im

Kreis Heinsberg benannt wurde. Hier sollten die Teams den Vornamen und das Verwandtschaftsverhältnis angeben. „Ein paar Teams haben allerdings nur eins von beiden recherchiert“, sagt Hanna Höppler. Auch dafür konnte es keine volle Punktzahl geben.

Auch beim Sponsor des Netrace, dem Telekommunikationsanbieter NetAachen, wird der Verlauf des Wettbewerbs aufmerksam verfolgt. „Wir wünschen den verbleibenden 41 Teams gutes Gelingen und viel Durchhaltevermögen beim Lösen der Fragen“, sagt Pressesprecherin Hannah Lynn Hoffmann. Einen persönlichen Tipp hat sie auch: „Lieber eine Frage kurz ruhen lassen und dann mit frischem Kopf wieder dran gehen. Sorgfalt schlägt Schnelligkeit!“

Ab dem kommenden Dienstag, 6. Februar, haben die Teams Gelegenheit zu zeigen, dass sie die Vor- und die Hauptrunde genutzt haben, um sich zu perfektionieren: Dann beginnt das große Finale.



Vom Netrace-Konzept überzeugt: Lehrerin Beate Schreiber.

Für das Finale qualifizierte Teams



Schule	Team	Pkt.	Spielzeit
Berufskolleg Erkelenz	Fortnite Lover	46	00:00:01:56
Berufskolleg Ernährung Sozialwesen Technik	AbiDoppelGut	42	00:01:23:19
Berufskolleg Eschweiler	Braingame	43	00:00:58:43
Berufskolleg für Gestaltung und Technik	Error 404	35	04:06:53:20
Berufskolleg für Technik Düren	Die Gompelmaennchen	41	02:00:49:29
Berufskolleg für Wirtschaft und Verwaltung	ThePower	11	06:09:36:16
Berufskolleg Jülich	Die sechs 7 Weisen	0	00:07:34:12
Berufskolleg Wirtschaft des Kreises Heinsberg	Team ohne Namen	47	06:10:38:37
Bischöfliche Marienschule / Projekt MOTIVIA	MOTIVIANER	46	00:06:24:23
Burgau-Gymnasium	Die Quietschfidelen	39	00:04:00:56
Einhard-Gymnasium	WebRacer	41	00:02:00:23
Elisabethschule	Batman	6	00:01:28:24
Franziskus Gymnasium Vossenack	FGV Sparta	46	00:00:45:12
Ganztagshauptschule Hückelhoven	Medienscouts	28	04:08:16:21
Gesamtschule Würselen	Kurs 10if Team 3	50	04:10:44:27
Goethe Gymnasium Stolberg	salatigesSenfgemuese-brot	43	01:23:21:10
Goltstein-Schule Inden	LePiSa	35	01:18:44:16
Gymnasium am Wirteltor	auf_Lock	42	00:01:33:15
Gymnasium der Stadt Alsdorf	Dalton14	33	00:02:22:52
Gymnasium Hückelhoven	Die TorPedros	42	00:01:58:12
Hugo-Junkers-Realschule	HJR-Scouts	50	00:05:05:37
Inda-Gymnasium Aachen	Internet Explorer	32	00:00:50:00
Käthe-Kollwitz-Schule Herzogenrath	No.Brain.No.Game	19	00:05:23:20
Kupferstädter Gesamtschule Stolberg	KogelStreetNews	49	00:12:33:16
Luise-Hensel-Realschule Aachen	dumm dogs	14	00:02:49:06
Mädchengymnasium Jülich	Die sieben Zwerge	21	00:01:36:15
Maria Montessori Gesamtschule Aachen	Monte 8d	0	07:00:00:00
Maria-Sibylla-Merian Gesamtschule	Melody	16	00:02:27:02
Peter-Jordan-Schule	pjs-heroes	44	00:20:09:08
Pius-Gymnasium	if-anweisung.de	41	00:01:11:52
Realschule Baesweiler	Semmelbroetchen	29	05:07:25:31
Realschule Heinsberg	Delay Hardstuck	40	04:23:16:41
Rurtal Gymnasium Düren	Rurtaler 1	46	00:01:52:28
Sekundarschule Kreuzau/Nideggen	7 vs. Computer	18	00:05:00:12
St Ursula Aachen	Baddies	39	00:02:58:00
Städtisches Gymnasium Eschweiler	A-Team	40	00:01:28:04
Städtisches Gymnasium Würselen	Angry Nerds	31	00:01:38:49
Stiftisches Gymnasium Düren	Stift	50	04:22:42:05
Viktor Frankl Schule	HackerGeneration	33	00:03:04:49
Viktoriaerschule Aachen	W-laaan	36	00:01:50:11
Waldschule Eschweiler	6b Superheroes	31	05:06:34:10

QUELLE: AZAN-NETTRACE.DE

Neuer iPhone-Schutz lässt Langfinger alt aussehen

PIN-Code allein reicht nicht mehr, um Daten zu sehen.

BERLIN iPhone- oder iPad-Diebe spähen oft den PIN-Code eines Gerätes aus, bevor sie es stehlen. Dann haben sie freien Zugang zum Telefon und allen Daten in der iCloud. Dem lässt sich nun ein Riegel verschieben. Denn per Software-Update hat Apple eine neue Schutzfunktion auf iPhones und iPads gebracht. Sie sorgt dafür, dass der PIN-Code allein nicht mehr reicht, um auf sensible Daten zuzugreifen, wenn sich das Gerät nicht an vertrauten Orten wie daheim oder am Arbeitsplatz befindet. „So soll verhindert werden, dass eine Person, die dein Gerät gestohlen hat und deinen Code kennt, wichtige Änderungen an deinem Account oder Gerät vornimmt“, erklärt Apple die neue, zusätzliche Schutzebene.

Nicht ohne Biometrie

Aktionen wie etwa der Zugriff auf gespeicherte Passwörter im iCloud-Schlüsselbund oder auf gespeicherte Kreditkarten erfordern dann eine weitere, biometrische Authentisierung mit Face- oder Touch-ID, also einen Gesicht- oder Fingerabdruck-Scan. Eine zweite Komponente der neuen Schutzfunktion ist eine Verzögerung bei sicherheitsrelevanten Ak-

tionen: Soll beispielsweise das Apple-ID-Passwort geändert werden, muss zunächst eine Stunde gewartet werden, anschließend ist ebenfalls wieder ein Gesicht- oder Fingerabdruck-Scan notwendig.

Um die neue Schutzfunktion unter „Einstellungen/Face ID & Code/(Gerätecode eingeben)/Schutz für gestohlene Geräte“ aktivieren zu können, muss die Zwei-Faktor-Authentisierung für die Apple-ID verwendet werden. Zudem gilt es, Folgendes auf dem Gerät zu aktivieren: Gerätecode, Face- oder Touch-ID, „Wo ist?“ sowie „Wichtige Orte“ (Ortungsdienste).

Aufs Gerät kommt das Feature mit der neuen iOS-Version 17.3, die auch viele Sicherheitslücken schließt. Zeitgleich ist die neue MacOS-Version 14.3 veröffentlicht worden, die diverse Sicherheitsprobleme auf Apple-Rechnern behebt.

Für gewöhnlich sollte man die Updates auf iPhones, iPads sowie Mac-Notebooks und -Desktoprechnern zu Installation angeboten bekommen. Falls das nicht geschieht, lässt sich die Aktualisierung in den Einstellungen (iPhones und iPads) beziehungsweise in den Systemeinstellungen (Mac) unter „Allgemein/Softwareupdate“ starten. (dpa)

Erbeuteten Passwörtern auf der Spur

Account gehackt? Dann gilt es, möglichst schneller zu sein als potenzielle Angreifer.

BERLIN Hackerangriffe und Datenlecks spülen täglich unzählige Kombinationen aus Benutzernamen und Passwörtern ins Netz. Für Betroffene heißt es: Möglichst schneller sein als potenzielle Angreifer. Was in den Tiefen des Internets an kompromittierten Log-in-Daten für Konten und Dienste zu finden ist, sammelt der australische Sicherheitsforscher Troy Hunt in einer Datenbank.

Nutzer können die sensible Sammlung kostenlos auf der Seite „Have I been pwned?“ (Sinngemäß: Hat es mich erwischt?) abfragen, um sich genau diese Frage zu beantworten. Dazu muss man nur eine oder mehrere E-Mail-Adressen, die man als Benutzernamen für Konten nutzt, zur Abfrage eingeben.

Neue Identitätsdaten

Selbst für alle, die die Seite kennen und schon einmal genutzt haben, gilt: Ein regelmäßiger Besuch lohnt sich. Erst jüngst hat Hunt wieder einen neuen, 104 Gigabyte schweren Datensatz mit mehr als 70 Millionen E-Mail-Adressen zur Datenbank hinzugefügt. Und auch wenn es Überschneidungen in den Datenbeständen geben wird, lohnt es sich, parallel ein weiteres kostenloses Abfrage-An-

gebot zu nutzen: den Identity Leak Checker des Hasso-Plattner-Instituts (HPI). Auch der Checker baut auf einer Datenbank auf, die zahllose bloßgestellte Identitätsdaten enthält.

Ergeben die Abfragen auf einer der Seiten Treffer, gilt es, das verbrannte Passwort beim jeweiligen Dienst schnell durch ein neues, sicheres Passwort zu ersetzen.

Ein Passwortmanager

Wichtig: Es muss ein individuelles

Passwort für jeden Dienst sein. Dasselbe Passwort für viele oder gar alle Dienste zu verwenden, ist riskant. Denn damit haben Angreifer leichtes Spiel und können viele oder alle Konten im Handstreich übernehmen.

Weil sich niemand Dutzende komplizierte Passwörter merken kann, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz von Passwortmanagern. Alternativ dazu kann man auch mithilfe eines Passwortmerkblatts sicherer im Netz unterwegs sein - die Me-

thode dahinter erläutert das BSI auf seiner Website.

Doppelt schützt besser

Zudem sollte man bei Online-Diensten die Zwei-Faktor-Authentisierung (2FA) aktivieren, wo immer sie verfügbar ist. Denn dank eines zweiten Codes, der hier beim Log-in abgefragt wird, kommen potenzielle Angreifer selbst dann nicht ins jeweilige Konto, wenn sie das Passwort erbeutet haben sollten. (dpa)



Nicht zu einfach denken: Passwörter wie die Tastaturfolge asdfghjk scheinen zwar komplex, sind aber einfach zu erraten. Das gilt erst recht für das sehr beliebte 123456. FOTO: DPA