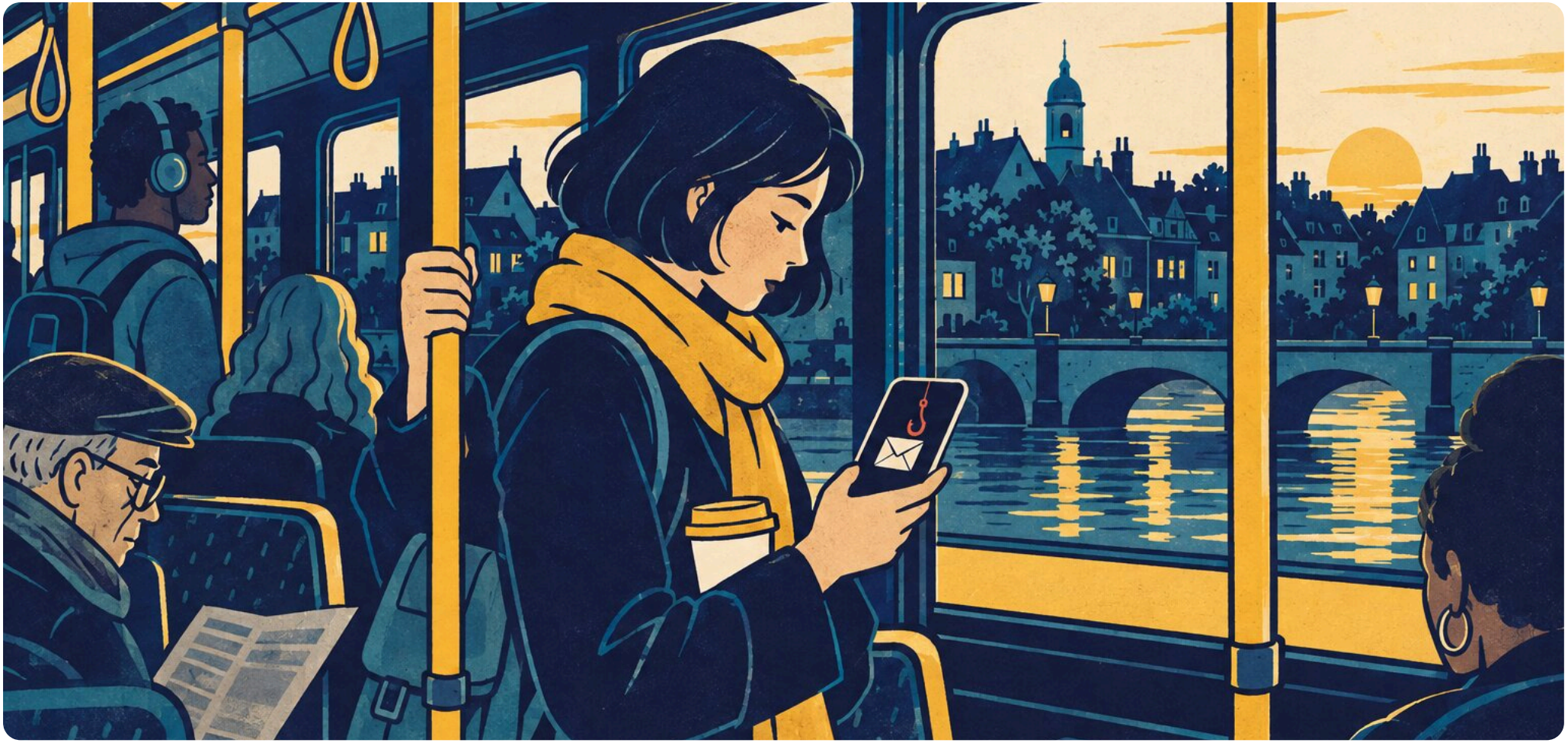


RUNDE 1 · TAG 0 · DONNERSTAG, 18:42 UHR

Der Köder

FRAGE ANS TEAM

So etwas kann jedem an einem langen Tag passieren. Was habt ihr, damit so ein Link wenig Schaden anrichtet?

- **Hanne fragt:** Würde ich so eine Mail erkennen? Hat mir das beim Verein je jemand gezeigt?
- **Katrin fragt:** Mein Postfach war der Anfang. Wer hätte mich warnen können, und wie schnell?
- **Und bei uns:** Wo melden wir uns unterwegs am Handy an, zwischen zwei Terminen?

RUNDE 1 · TAG 0 · DONNERSTAG, 18:42 UHR · 8 MINUTEN

Der Köder

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Mira fährt Straßenbahn, Linie 4, kurz hinter dem Marktplatz. Sie steht und hat das Handy in der Hand. Es war ein langer Tag. Sie hat zwei neue Lesepatinnen eingewiesen. Das Herbstferienprogramm ist zu drei Vierteln voll. Für das Sprachcafé am Mittwoch bringt noch niemand Kuchen.

Das Handy vibriert. Eine Mail von Katrin, Schulsozialarbeiterin an der Auenschule. Betreff: „Anmeldeliste Herbstferien – bitte heute noch bestätigen“. Darunter zwei Zeilen, wie Katrin immer schreibt, und ein Link: „Liste öffnen“.

Mira tippt auf den Link. Eine Seite geht auf. Sie sieht aus wie die Anmeldung ihres Mail-Anbieters. Komisch, denkt Mira, ich war doch angemeldet. Die Bahn bremst, jemand drängt vorbei. Mira tippt das Passwort des Vereinspostfachs ein. Dann steht da: „Die Datei wurde nicht gefunden.“

Mira steckt das Handy weg. Morgen im Büro, denkt sie. Am Lindenplatz steigt sie aus.

Mira weiß nicht: Seit gestern ist ein Angreifer in Katrins Postfach. Die Mail kam wirklich von Katrins Adresse. Aber geschrieben hat sie der Angreifer.

FRAGE ANS TEAM

So etwas kann jedem an einem langen Tag passieren. Was habt ihr, damit so ein Link wenig Schaden anrichtet?

2 Beraten 2 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir“ daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 2 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

Keine Karte. Irgendwann klickt jemand auf so einen Link, müde oder in Eile. Ganz verhindern lässt sich das nicht.

MACHT DEN SCHADEN KLEINER

17 Betrugs-Mails erkennen

Mira kennt die Regel: Nie über einen Link aus einer Mail anmelden. Sie hätte die Seite geschlossen und Katrin angerufen.

11 Passwort-Manager

Der Passwort-Manager setzt das Passwort nur auf der echten Seite ein. Hier hätte er nichts getan, und Mira hätte gestutzt.

18 Probleme sofort melden

„Datei nicht gefunden“ nach einer Anmeldung ist seltsam. Mira hätte der Notfallperson kurz geschrieben. Das Passwort wäre noch am Abend geändert worden.

HILFT HIER NICHT

- **Absender prüfen, Spamfilter:** Die Mail kam von Katrins echter Adresse. Kein Filter merkt etwas.
- **Ein langes, starkes Passwort:** Niemand hat es erraten. Mira hat es selbst eingetippt.

4 Schaden 1 Min.

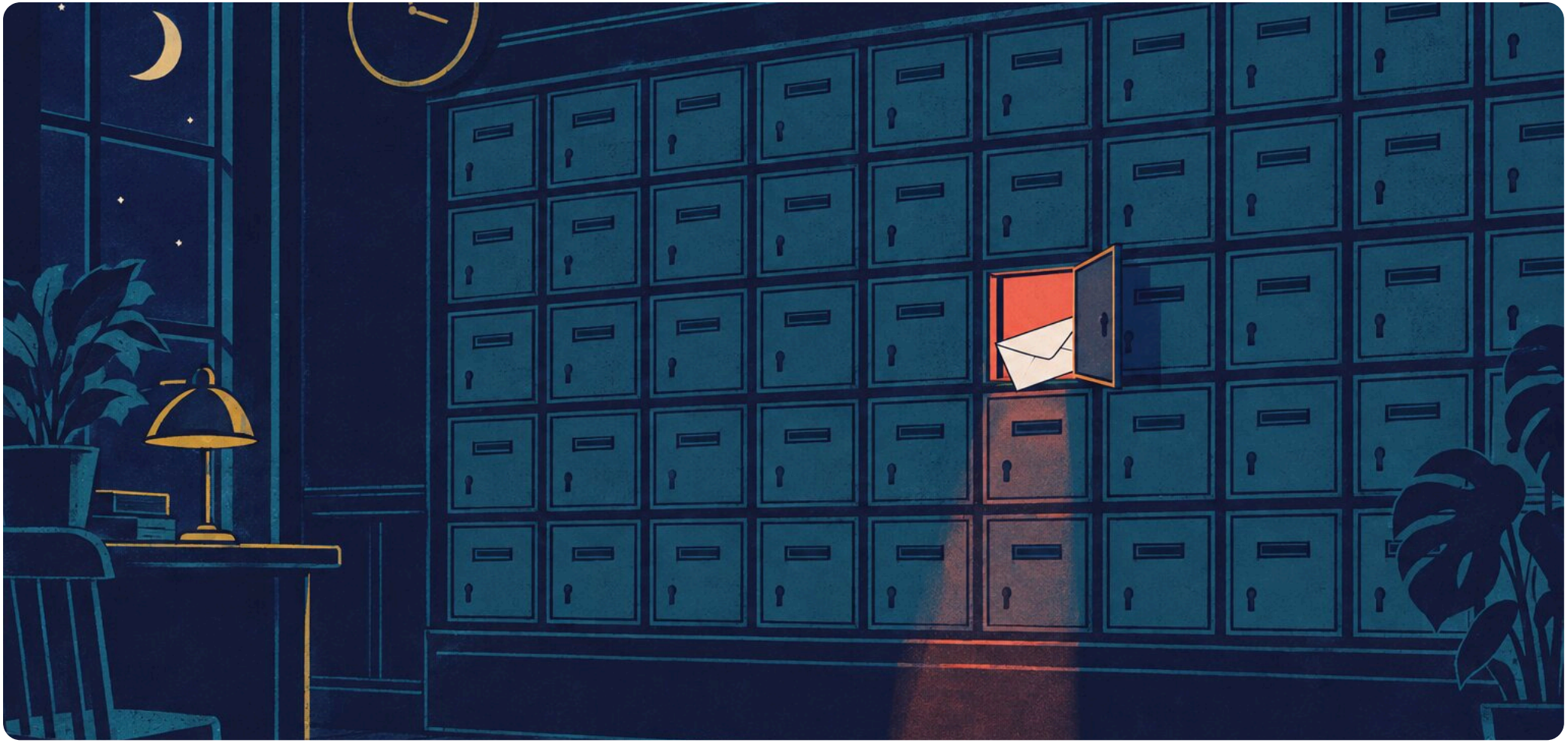
1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Ihr habt es dem Angreifer schwer gemacht. Meistens reicht das. Heute leider nicht. Er hat das Passwort.

3 **Ihr habt keine dieser Karten.** Der Angreifer hat das Passwort. Niemand ahnt etwas. Mira schläft gut.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“. Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Die Mail kam wirklich aus Katrins Postfach. So eine Mail erkennt kein Spamfilter. Auch geschulte Leute klicken manchmal darauf. Darum ist im Spiel wichtig, was danach passiert.



RUNDE 2 · TAG 1 · FREITAG, 02:13 UHR

Die zweite Anmeldung

FRAGE ANS TEAM

Das Passwort allein hat gereicht. Was habt ihr, das diese Anmeldung verhindert oder euch gewarnt hätte?

- **Hanne fragt:** Leitet ihr die Vereinspost eigentlich auch an private Adressen weiter? An meine?
- **Katrin fragt:** Wer von euch würde merken, dass nachts jemand im Postfach war?
- **Und bei uns:** Wer kennt das Passwort für unser wichtigstes Postfach? Wann hat zuletzt jemand die Weiterleitungen geprüft?

RUNDE 2 · TAG 1 · FREITAG, 02:13 UHR · 12 MINUTEN

Die zweite Anmeldung

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Auenbrück schläft. Im Büro in der alten Feuerwache ist es dunkel. Miras Handy lädt auf dem Nachttisch.

Irgendwo meldet sich jemand an, weit weg oder zwei Straßen weiter. Mit der Adresse kontakt@weitersagen-auenbrueck.example und dem Passwort, das Mira gestern in der Bahn eingetippt hat.

Das Postfach öffnet sich. 14.212 Nachrichten.

Der Angreifer liest noch nichts. Zuerst ändert er die Einstellungen. Ab jetzt geht von jeder neuen Mail eine Kopie an eine fremde Adresse. Mails mit „Sicherheit“ oder „Anmeldung“ im Betreff landen ungelesen im Archiv. So sieht Mira keine Warnungen.

Um 02:19 Uhr meldet er sich ab. Er hat nichts gelöscht. Am Morgen sieht das Postfach aus wie immer.

Ab jetzt liest jemand mit.

FRAGE ANS TEAM

Das Passwort allein hat gereicht. Was habt ihr, das diese Anmeldung verhindert oder euch gewarnt hätte?

2 Beraten 4 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir“ daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 3 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

8 Passkey fürs Postfach

Mit Passkey meldet sich Mira über ihr Handy an, ohne Passwort. Ohne das Handy kommt niemand ins Postfach. Auf der falschen Seite geht der Passkey gar nicht.

MACHT DEN SCHADEN KLEINER

9 Anmelde-Code per App

Das Passwort allein reicht nicht mehr. Der Angreifer braucht auch den Code aus Miras App. Manche falschen Seiten fragen den Code gleich mit ab. Aber nicht alle können das.

12 Postfach-Einstellungen prüfen

Vielleicht sieht Mira morgens die Warnung „Neues Gerät angemeldet“. Spätestens beim monatlichen Blick in die Einstellungen fällt die Weiterleitung auf. Der Angreifer hat Tage statt Monate.

HILFT HIER NICHT

- **Ein langes Passwort, nur für dieses Konto:** Es schützt eure anderen Konten. Hier nicht, denn Mira hat es selbst eingegeben.
- **Virenschutz:** Auf euren Geräten ist kein Virus. Der Angreifer meldet sich ganz normal an, wie ihr auch.

4 Schaden 1 Min.

0 **Ihr habt Karte 8.** Die Anmeldung klappt nicht. Der Angreifer versucht es dreimal. Dann geht er zum nächsten Verein auf der Liste. **Der Angriff ist gestoppt.**

1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Der Angreifer kommt hinein, aber nur mit Mühe und nicht für lange. Was er in dieser Zeit findet, zeigt die nächste Runde.

3 **Ihr habt keine dieser Karten.** Der Angreifer kommt jederzeit ins Postfach. Er bekommt eine Kopie jeder neuen Mail. Das bleibt so, auch wenn Mira ihr Passwort ändert.

Hat das Team Karte 8, lies vor:

Der Angriff ist gestoppt. Das ist die stärkste Karte im Spiel, und ihr habt sie. Wir spielen trotzdem weiter. Die privaten Postfächer eurer Ehrenamtlichen schützt euer Passkey nicht. Was wäre, wenn der Angreifer dort hineinkommt? Ab jetzt legen wir die Marken in die zweite Zeile.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“. Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Ein Passkey funktioniert nur auf der echten Seite. Auf einer falschen Seite kann ihn niemand stehlen. Einen Code aus einer App oder per SMS kann ein Angreifer dagegen sofort mit abfragen. Eine heimliche Weiterleitung bleibt auch nach einem neuen Passwort bestehen.



RUNDE 3 · TAG 2 BIS 4 · SAMSTAG BIS MONTAG

Die Fundgrube

FRAGE ANS TEAM

Der Angreifer ist schon im Postfach. Was habt ihr, damit dort weniger zu finden ist?

- **Katrin fragt:** Wissen die Eltern eigentlich, wie lange ihr die Bögen aufhebt und wer sie alles bekommt?
- **Hanne fragt:** Meine Notizen nach den Lesestunden schicke ich seit Jahren per Mail. Liegen die alle noch da?
- **Und bei uns:** Stellt euch vor, jemand sucht in unserem Postfach nach „Anmeldung“, „Attest“ oder „Passwort“. Was fände er? Nur in Gedanken, kein Gerät öffnen.

RUNDE 3 · TAG 2 BIS 4 · SAMSTAG BIS MONTAG · 12 MINUTEN

Die Fundgrube

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Angriff in Runde 2 gestoppt? *Dann lies zuerst: „Diesmal ist es Hannes privates Postfach. Dorthin schickt ihr seit Jahren Bögen und Notizen. „Euer Postfach“ heißt hier: ihres.“*

Der Angreifer hat das ganze Wochenende Zeit. Er benutzt das Suchfeld in eurem Postfach.

Er sucht nach „Anmeldung“. 412 Treffer. Das sind die Bögen fürs Ferienprogramm aus 6 Jahren. Auf jedem steht ein Kind mit Namen und Geburtsdatum. Unten ist das Feld „Was wir wissen sollten“. Dort schreiben Eltern: Asthmaspray im Rucksack. Tabletten gegen Anfälle. „Darf auf keinen Fall vom Vater abgeholt werden.“

Er sucht nach „Notiz“. Nach jedem Treffen schreiben die Lernpatinnen und Lesepaten Mira ein paar Zeilen. Wie es dem Kind geht. Dass es zu Hause schwierig ist. Dass ein Brief vom Amt seit Wochen ungeöffnet auf dem Küchentisch liegt.

Er sucht nach „Führungszeugnis“. 11 Treffer, alle eingescannt und gut lesbar.

Er sucht nach „Passwort“. Auch da findet er etwas.

Nichts davon hat je jemand gelöscht. Der Speicher war ja nie voll.

Am Montagmorgen hat der Angreifer 1.900 Dateien kopiert. Mira beantwortet gerade die Mails vom Wochenende.

FRAGE ANS TEAM

Der Angreifer ist schon im Postfach. Was habt ihr, damit dort weniger zu finden ist?

2 Beraten 4 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir“ daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 3 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

Keine Karte. Der Angreifer kann alles lesen, was im Postfach liegt. Hier hilft nur, was ihr vorher getan habt.

MACHT DEN SCHADEN KLEINER

1 Weniger abfragen

Der Bogen hätte kein Feld „Was wir wissen sollten“. Hinweise kämen ohne Namen: „1 Kind mit Asthma, die Betreuerin weiß Bescheid.“

2 Sicherer Ordner statt Mail

Bögen und Notizen lägen in einem geschützten Ordner, nicht im Postfach. In der Mail stünde nur: „Neuer Bogen liegt im Ordner.“

3 Regelmäßig löschen

Statt 6 Jahren lägen nur die letzten 6 Wochen im Postfach. Der Angreifer fände nur das laufende Ferienprogramm.

HILFT HIER NICHT

- **Passkey, Anmelde-Code, Passwort-Manager:** Sie schützen die Anmeldung. Der Angreifer ist aber schon drin.
- **„Das geben uns die Eltern doch freiwillig“:** Das stimmt. Trotzdem seid ihr verantwortlich, sobald es bei euch liegt.

4 Schaden 1 Min.

1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Der Angreifer findet etwas. Aber er findet keine 6 Jahre und nicht alles an einem Ort. Nur wenige Familien sind betroffen.

3 **Ihr habt keine dieser Karten.** Der Angreifer hat Daten aus 6 Jahren kopiert, über Kinder, Krankheiten und Familien. Nichts davon lässt sich zurückholen.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“. Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Wenig Daten und regelmäßiges Löschen helfen auch dann, wenn jemand schon im Postfach ist. Angaben zur Gesundheit sind besonders geschützt, auch wenn Eltern sie freiwillig geben. Führungszeugnisse schaut ihr nur an und notiert, wann ihr sie gesehen habt. Kopien oder Scans dürft ihr nicht aufheben.



RUNDE 4 · TAG 4 · MONTAG, 23:40 UHR

Offene Türen

FRAGE ANS TEAM

Über das Postfach kam der Angreifer in alle Konten. Was habt ihr, damit er dort nicht hineinkommt oder wenig findet?

- **Hanne fragt:** Steht meine Adresse bei euch in einer Tabelle? Wer kann die öffnen?
- **Katrin fragt:** Wer von euch könnte heute alle Dienste aufzählen, die der Verein nutzt?
- **Und bei uns:** Wohin schickt „Passwort vergessen“ bei uns den Link? Kennt jemand ein Passwort, der längst nicht mehr dabei ist?

RUNDE 4 · TAG 4 · MONTAG, 23:40 UHR · 12 MINUTEN

Offene Türen

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Angriff in Runde 2 gestoppt? *Dann lies zuerst: „Diesmal ist es Hannes Postfach. Von euch liegen darin Ordner-Links, ein weitergeleitetes Passwort und die Liste der Ehrenamtlichen.“*

Fast jedes Konto des Vereins ist mit dem Postfach verbunden.

Der Angreifer öffnet die Anmeldung eurer Cloud, eures Online-Speichers. Er klickt auf „Passwort vergessen“. Nach 10 Sekunden ist der Link im Postfach. Er setzt ein neues Passwort und ist im Ordner „Verein“.

Darin liegt die Tabelle „Ehrenamt_aktuell“. 43 Zeilen: Name, Handynummer, Wohnadresse, Kontonummer für die Fahrtkosten. Zeile 17: Hanne, 74, Lesepatin seit 9 Jahren, Am Mühlgraben 6.

In einer Mail von 2023 hatte der Angreifer schon gelesen: „Hier das Passwort fürs Instagram, bitte nicht weitergeben :)“. Es funktioniert noch. 3 Leute, die es kannten, sind inzwischen gegangen.

Bei der Website und beim Rundbrief mit 600 Adressen klappt das genauso.

Nach 20 Minuten ist er in allen Konten des Vereins. Die Mails mit den Links löscht er wieder.

FRAGE ANS TEAM

Über das Postfach kam der Angreifer in alle Konten. Was habt ihr, damit er dort nicht hineinkommt oder wenig findet?

2 Beraten 4 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir“ daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 3 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

10 Anmelde-Code für alle Konten

„Passwort vergessen“ reicht nicht. Cloud, Website und Rundbrief wollen auch einen Code aus einer App. Der kommt nicht per Mail. Das alte Instagram-Passwort allein nützt nichts.

MACHT DEN SCHADEN KLEINER

13 Liste aller Konten

Ihr wisst, welche Konten es gibt und an welchem Postfach jedes hängt. Die wichtigsten hängen am sichersten Postfach, nicht an kontakt@.

6 Wohnadressen schützen

Die Tabelle hat Namen und Handynummern, aber keine Wohnadressen. Niemand erfährt, wo Hanne wohnt.

4 Zugriff begrenzen

Mit dem Konto der Koordination sieht man nur das Nötige. Keine Tabelle ist über einen offenen Link erreichbar, der in einer alten Mail steht.

5 Zugänge beim Austritt sperren

Das Instagram-Passwort wäre seit 2023 dreimal geändert worden. Immer, wenn jemand gegangen ist.

11 Passwort-Manager

Das Passwort stünde im Passwort-Manager und in keiner Mail. Die Suche nach „Passwort“ bliebe leer.

HILFT HIER NICHT

- **Der Passkey fürs Postfach:** Er hätte den Angriff in Runde 2 gestoppt. Jetzt ist es dafür zu spät.
- **Ein Code, der per Mail kommt:** Er landet in dem Postfach, das der Angreifer gerade liest.

4 Schaden 1 Min.

0 **Ihr habt Karte 10.** Der Angreifer versucht es bei 4 Konten. Er kommt in keines hinein. Er hat nur das Postfach.

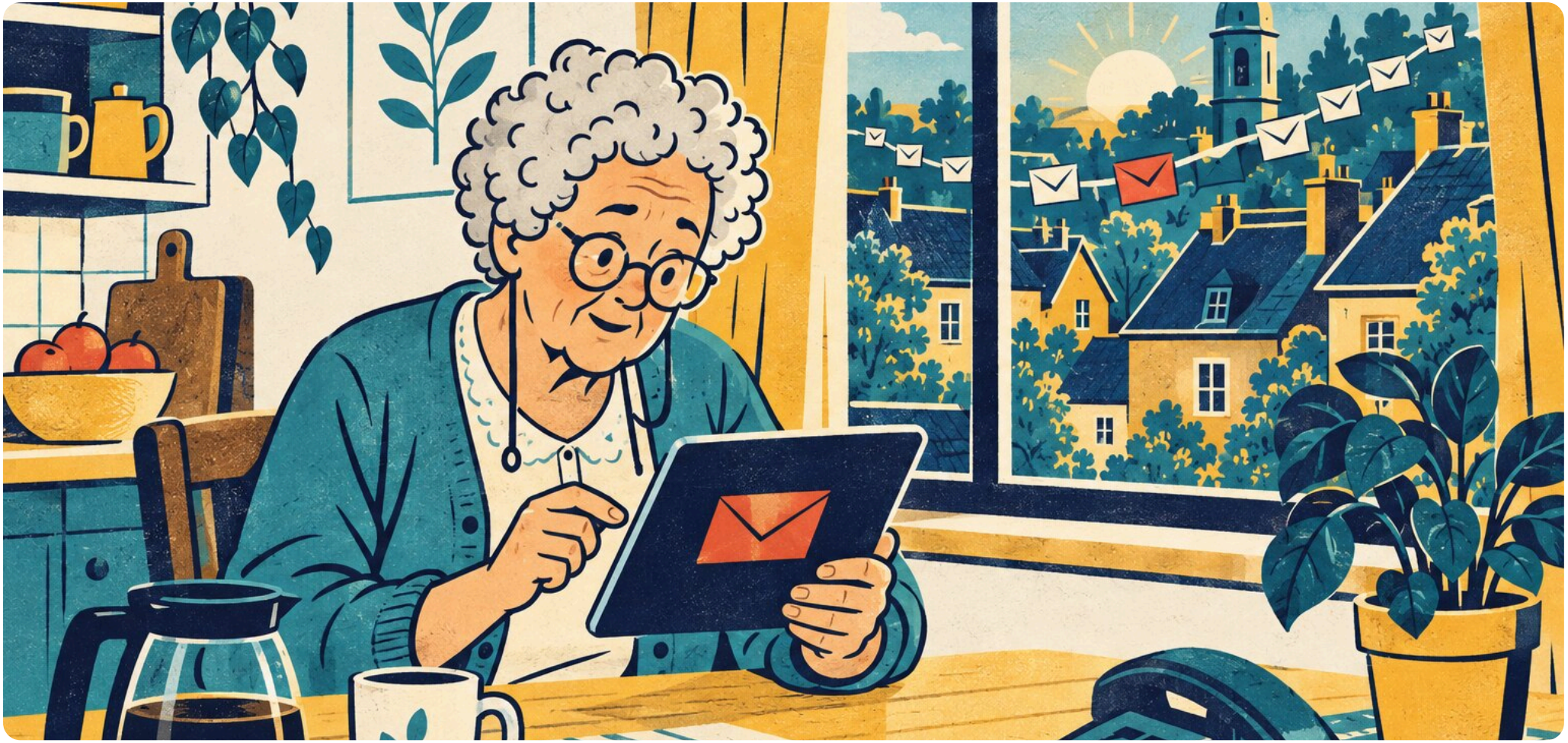
1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Der Angreifer kommt in einige Konten. Er findet dort aber weniger als erhofft.

3 **Ihr habt keine dieser Karten.** Der Angreifer hat jetzt Cloud, Website, Rundbrief und Instagram. Und er hat die Wohnadressen von 43 Menschen.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“. Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Fast jeder Dienst schickt bei „Passwort vergessen“ einen Link ans Postfach. Wer das Postfach hat, kommt so in viele Konten. Ein Anmelde-Code per App verhindert das. Wenn jemand den Verein verlässt, ändert ihr die Passwörter, die er kannte.



RUNDE 5 · TAG 5 · DIENSTAG, 07:30 UHR

Stille Post

FRAGE ANS TEAM

Diesmal trifft es Leute, die euch vertrauen. Was habt ihr, damit sie eine falsche Mail erkennen und ihr sofort davon erfahrt?

- **Hanne fragt:** Woran erkenne ich, dass eine Mail nicht wirklich von euch ist? Und wen rufe ich dann an?
- **Katrin fragt:** Wie warnt ihr uns Partner, ohne das betroffene Postfach zu benutzen?
- **Und bei uns:** Wissen unsere Leute, dass wir nie nach Passwörtern fragen? Haben wir es ihnen je gesagt?

RUNDE 5 · TAG 5 · DIENSTAG, 07:30 UHR · 12 MINUTEN

Stille Post

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Angriff in Runde 2 gestoppt? *Dann lies zuerst: „Die falsche Mail kommt diesmal von Hannes Adresse, an alle aus euren Rundmails."*

Hanne sitzt am Küchentisch, der Kaffee läuft durch. Ihre Enkelin hat ihr das Tablet eingerichtet. Dort ist eine neue Mail vom Verein. Absender: kontakt@weitersagen-auenbrueck.example. Betreff: „Neue Einsatzliste – bitte bis Freitag eintragen". Darunter: „Liebe Grüße, Mira".

Die Mail kommt wirklich aus eurem Postfach, mit eurer Adresse und eurem Logo. Geschrieben hat sie der Angreifer. Sie geht an alle 43 Ehrenamtlichen, an die Auenschule, die Stadtbibliothek und das Jugendamt.

Der Link führt zu einer Anmeldeseite. Hanne wundert sich nicht. Für die Einsatzliste musste sie sich schon immer anmelden. Sie setzt die Brille auf und tippt ihr Passwort ein. Es ist dasselbe wie für ihr eigenes Postfach.

Bis zum Mittag haben 19 Menschen den Link geöffnet. Sieben haben ein Passwort eingegeben. Zwei von ihnen arbeiten an Schulen.

Genau so hat es vor einer Woche bei Katrin angefangen. Jetzt verschickt der Angreifer Mails in eurem Namen.

FRAGE ANS TEAM

Diesmal trifft es Leute, die euch vertrauen. Was habt ihr, damit sie eine falsche Mail erkennen und ihr sofort davon erfahrt?

2 Beraten 4 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir" daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 3 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

Keine Karte. Die Mail kommt wirklich von euch. Kein Filter hält sie auf. Jetzt hilft nur, was eure Leute wissen.

MACHT DEN SCHADEN KLEINER

16 Echte Mails von uns erkennen

Hanne weiß: Der Verein fragt nie per Mail nach einem Passwort. Sie hat eine Nummer, die sie anruft, wenn etwas komisch ist.

21 Ehrenamtliche einweisen

Alle Ehrenamtlichen haben 3 Regeln unterschrieben. Eine davon heißt: „Verdacht sofort melden." Sie wissen, dass ihr das wollt.

18 Probleme sofort melden

Um 07:45 Uhr ruft jemand die Notfallperson an: „Habt ihr mir gerade geschrieben?" So erfahrt ihr es am 5. Tag und nicht erst aus dem Netz.

17 Betrugs-Mails erkennen

Auch die Ehrenamtlichen hatten die jährliche Schulung. Alle wissen: Nie über einen Link aus einer Mail anmelden.

HILFT HIER NICHT

- **Technische Absender-Prüfung (Karte 16, letzter Schritt):** Diese Mail ist nicht gefälscht. Sie kommt wirklich aus eurem Postfach.
- **Eine Warnung per Rundmail aus demselben Postfach:** Der Angreifer liest mit. Er kann eure Warnung löschen oder beantworten.

4 Schaden 1 Min.

1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Einige klicken trotzdem. Aber jemand ruft an. Ihr erfahrt heute, dass etwas nicht stimmt. Damit gewinnt ihr 10 Tage.

3 **Ihr habt keine dieser Karten.** Niemand ruft an. Der Angreifer hat jetzt 7 weitere Postfächer, 2 davon an Schulen. Von dort schickt er die nächsten falschen Mails los, mit eurem Namen darin.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht" liegen, kommen auf das Feld „Plan". Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Wer ein Postfach übernimmt, schreibt fast immer dessen Kontakte an. Die Leute vertrauen dem bekannten Absender. Dann hilft nur, auf einem anderen Weg nachzufragen, zum Beispiel per Telefon. Und alle müssen wissen, dass Melden erwünscht ist.



RUNDE 6 · TAG 15 · FREITAG, 16:50 UHR

Die Schlagzeile

FRAGE ANS TEAM

Jetzt ist alles öffentlich. Was habt ihr, damit ihr in der ersten Stunde schnell handeln könnt und eure Leute geschützt sind?

- **Hanne fragt:** Wer von euch ruft mich an diesem Abend an? Und was kann ich tun, wenn jemand vor meinem Haus steht?
- **Katrin fragt:** Was sagt ihr der Mutter am Telefon? Wer von euch sagt es?
- **Und bei uns:** Wer spricht bei uns nach außen, und wer weiß das?

RUNDE 6 · TAG 15 · FREITAG, 16:50 UHR · 12 MINUTEN

Die Schlagzeile

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Angriff in Runde 2 gestoppt? *Dann lies zuerst: „Diesmal stammt alles im Blog aus Hannes Postfach. Ihr hattet es ihr geschickt.“*

Leos Handy summt immer wieder. Jemand hat einen Link in die Gruppe gestellt. Er führt zur „Auenwacht“. Dieser Blog schreibt seit dem Sommer gegen das Sprachcafé. Der neue Artikel heißt: „Was Weitersagen e. V. über Auenbrücker Kinder sammelt“.

Im Artikel stehen Auszüge aus Anmeldebögen. Die Namen sind schlecht geschwärzt. Dazu ein Satz aus der Notiz einer Lernpatin. Unter der Überschrift „Wer steckt dahinter?“ stehen 43 Namen. Nach einer Stunde stehen in den Kommentaren die ersten Adressen.

Um 17:20 Uhr ruft eine Mutter an. Sie ist sehr ruhig. Sie will wissen, wer jetzt alles weiß, wo ihre Tochter die Ferien verbringt.

Um 18:05 Uhr ruft die Lokalzeitung an. Um 18:30 Uhr schreibt die Auenschule: Die Zusammenarbeit ruht, bis das geklärt ist.

Um 19:10 Uhr steht ein Mann vor dem Haus Am Mühlgraben 6 und fotografiert das Klingelschild. Hanne steht hinter der Gardine.

Wer der Angreifer war, erfahrt ihr nie. Was er gefunden hat, kann jetzt jeder lesen.

FRAGE ANS TEAM

Jetzt ist alles öffentlich. Was habt ihr, damit ihr in der ersten Stunde schnell handeln könnt und eure Leute geschützt sind?

2 Beraten 4 Min.

Leg das Blatt mit dem Bild nach oben in die Mitte. Das Team legt Karten aus „Haben wir“ daneben. Die Gesprächsfragen stehen vorn.

3 Auflösen 3 Min.

Nimm das Blatt wieder auf und lies vor.

STOPPT DEN ANGRIFF

Keine Karte. Kopierte Daten holt niemand zurück. Ihr könnt nur noch beeinflussen, wie ihr reagiert und wie hart es eure Leute trifft.

MACHT DEN SCHADEN KLEINER

19 Notfallkarte

Ihr wisst, wer entscheidet und wen ihr anruft. Um 18 Uhr sucht niemand nach einer Telefonnummer.

20 Eine Person spricht für uns

Eine Person spricht für den Verein. Alle anderen verweisen an sie. Nach 20 Minuten steht der erste Text: was passiert ist, was ihr jetzt tut.

6 Wohnadressen schützen

Die Liste nennt Namen, aber keine Adressen. Und ihr wisst, wie Hanne beim Meldeamt ihre Adresse sperren lässt.

HILFT HIER NICHT

- **Schweigen und abwarten:** Die Familien erfahren es dann vom Blog und nicht von euch.
- **Vom Blog Löschung verlangen:** Das ist richtig, aber es dauert. Kopien tauchen woanders wieder auf.

4 Schaden 1 Min.

1–2 **Ihr habt Karten, die den Schaden kleiner machen.** 3 minus 1 je Karte, mindestens 1. Es ist ein furchtbarer Abend. Aber ihr informiert die Familien vor der Zeitung. Eine Person spricht für euch. Die Schule ruft am Montag zurück.

3 **Ihr habt keine dieser Karten.** Vier Leute telefonieren durcheinander. Niemand weiß, wer entscheiden darf. Die Familien lesen es zuerst im Netz. Zwei Ehrenamtliche hören noch in derselben Woche auf.

5 Plan und Logbuch 2 Min.

Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“. Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

FALLS JEMAND FRAGT Wer wegen seines Ehrenamts bedroht wird, kann beim Meldeamt seine Adresse sperren lassen. Dann gibt das Amt sie nicht mehr heraus. Beratungsstellen wie HateAid helfen bei Hass und Drohungen im Netz. Betroffene Familien informiert ihr in klarer, einfacher Sprache.



ERNSTFALL · TAG 15 · FREITAG, 19:30 UHR

Der Angriff fliegt auf

1 Die erste Stunde

6 Streifen liegen durcheinander auf dem Tisch. Legt sie in die Reihenfolge, in der ihr handeln würdet. Ihr habt 3 Minuten.

2 Fünf Entscheidungen

Die Spielleitung liest 5 Sätze vor. Nach jedem Satz zeigen alle gleichzeitig: Daumen hoch heißt „stimmt“, Daumen runter „stimmt nicht“. Dann sagt sie die Lösung.

3 Was euch Zeit kostet

Fünf Karten, fünf Sanduhren: Für jede Karte, die euch fehlt, verliert ihr Zeit in den 72 Stunden.

ERNSTFALL · TAG 15 · FREITAG, 19:30 UHR · 15 MINUTEN

Der Angriff fliegt auf

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



› Vorlesen 2 Min.

Halte das Bild hoch oder zeig es am Beamer, dann lies vor.

Ihr sitzt zu viert im Büro in der alten Feuerwache: Gloria, Mira, Tobi und Leo. Auf dem Tisch stehen kalter Tee und 4 Handys. Sie klingeln ständig.

Tobi hat im Postfach eine Regel gefunden. Seit 15 Tagen schickt sie jede Mail an eine fremde Adresse. Jemand war im Postfach. Er hat Daten von Kindern, Eltern und Ehrenamtlichen.

Gloria schaut auf die Uhr über der Tür. Es ist 19:30 Uhr. Ihr müsst den Angriff der Datenschutzbehörde melden. Dafür habt ihr 72 Stunden, also bis Montag um 19:30 Uhr. Das Wochenende zählt mit.

Mira sagt leise: „Ich glaube, das war ich. In der Straßenbahn."

Gloria schüttelt den Kopf. „Das waren wir alle. Und jetzt machen wir es der Reihe nach."

1 Die erste Stunde 4 Min.

Leg die sechs Ernstfall-Streifen gemischt auf den Tisch, stell den Wecker auf drei Minuten und lies vor:

6 Streifen liegen durcheinander auf dem Tisch. Legt sie in die Reihenfolge, in der ihr handeln würdet. Ihr habt 3 Minuten.

Empfohlene Reihenfolge: **D – B – F – A – E – C**

- **D zuerst (Übernehmen):** Eine Person muss entscheiden. Sonst tun alle dasselbe oder keiner etwas. Ab dieser Uhrzeit laufen die 72 Stunden.
- **B, F und A gehören zusammen:** Ein neues Passwort allein reicht oft nicht. Bei vielen Anbietern bleibt der Angreifer angemeldet. Über die Weiterleitung bekommt er außerdem jede Mail. Fotografiert die Regeln, bevor ihr sie löscht. Die Fotos sind euer Beweis.
- **E und C:** Hier ist die Reihenfolge nicht so wichtig. Seid ihr genug Leute, macht beides zugleich.
- **Nicht dabei, aber wichtig:** Hat ein Gerät vielleicht einen Virus, arbeitet nicht weiter damit. Trennt es vom Netz und holt Hilfe.

2 Fünf Entscheidungen 6 Min.

Ich lese 5 Sätze vor. Nach jedem Satz zeigt ihr alle gleichzeitig: Daumen hoch für „stimmt", Daumen runter für „stimmt nicht". Dann löse ich auf.

1 „Dafür sind wir gar nicht zuständig. Die Daten kamen ja von den Eltern und von der Schule."

STIMMT NICHT Doch. Ihr nutzt die Daten für euren Verein. Also seid ihr verantwortlich, egal von wem sie kommen. Anders ist es nur, wenn ihr Daten allein im Auftrag von jemand anderem bearbeitet. Dann meldet ihr ihm den Vorfall sofort.

2 „Wir müssen das der Datenschutzbehörde melden."

STIMMT Ja. Für die Betroffenen gibt es ein Risiko. Also müsst ihr sofort melden, möglichst innerhalb von 72 Stunden. Zuständig ist die Datenschutzbehörde eures Bundeslands. Sie hat dafür ein Online-Formular. Nur wenn wohl kein Risiko besteht, müsst ihr nicht melden.

3 „Wir melden erst, wenn wir genau wissen, was alles weg ist."

STIMMT NICHT Nein. Meldet, was ihr wisst, und reicht den Rest später nach. Wochenenden und Feiertage zählen bei den 72 Stunden mit. Wer später meldet, muss erklären, warum.

4 „Wir müssen die Familien und die Ehrenamtlichen selbst informieren."

STIMMT Ja, und zwar sofort. Das Risiko für sie ist hoch. Es geht um Gesundheitsdaten von Kindern und um Adressen von Menschen, die angefeindet werden. Schreibt klar und einfach: was passiert ist, was das für sie heißen kann, was ihr tut und wen sie fragen können.

5 „Eine Anzeige bei der Polizei ist Pflicht."

STIMMT NICHT Nein, aber sinnvoll. Anzeige erstattet ihr über die Onlinewache eures Bundeslands. Die Zentrale Ansprechstelle Cybercrime (ZAC) eurer Landespolizei berät auch Vereine.

3 Was euch Zeit kostet 3 Min.

Sucht diese 5 Karten in eurem Stapel „Haben wir" und legt sie auf den Tisch. Für jede fehlende Karte legt ihr eine Marke auf eine Sanduhr. Dort verliert ihr in den 72 Stunden Zeit. Die fehlenden Karten kommen auf den Plan.

19 Notfallkarte
Ohne sie sucht ihr erst Telefonnummern. Und ihr müsst klären, wer entscheiden darf.

13 Liste aller Konten
Ohne sie wisst ihr nicht, welche Konten ihr sichern müsst. Eins vergesst ihr.

7 Wissen, welche Daten wir haben
Ohne sie könnt ihr der Behörde und den Familien nicht sagen, welche Daten betroffen sind.

20 Eine Person spricht für uns
Ohne sie schreibt ihr den ersten Text nachts zu viert. Und jede:r sagt der Zeitung etwas anderes.

18 Probleme sofort melden
Ohne sie erfahrt ihr auch von der nächsten falschen Mail zu spät.

*Leg zum Schluss die **Ernstfall-Karte** in die Mitte: neun Schritte für den echten Ernstfall.*



SCHLUSS · TAG 90 · EIN DIENSTAG, DREI MONATE SPÄTER

Tag 90

SCHLUSSRUNDE

Jede Person sagt einen Satz: Was nehme ich mit? Die Spielleitung als Letzte. Dann tragen alle den Termin für Tag 90 in den Kalender ein, bevor jemand geht.

UNSER TAG 90 IST AM

SCHLUSS · TAG 90 · EIN DIENSTAG, DREI MONATE SPÄTER · 5 MINUTEN

Tag 90

RÜCKSEITE
NUR FÜR DIE SPIELLEITUNG



1 Vorlesen 2 Min.

Halte das letzte Blatt hoch oder zeig es am Beamer. Dann lies vor. Danach wird nichts mehr aufgelöst.

90 Tage später. Im Büro in der alten Feuerwache hängt neben der Tür ein Blatt mit 2 Namen und 5 Telefonnummern. Der Schredder ist voll.

Der Anmeldebogen fürs Osterferienprogramm hat ein Feld weniger. Die Bögen vom Herbst sind überall gelöscht. In der Tabelle „Ehrenamt“ gibt es keine Spalte „Adresse“ mehr. Das Postfach ist mit einem Passkey geschützt. Tobi hat endlich aufgeschrieben, welche Konten der Verein hat. Es sind 19.

An einem Donnerstag bekommt Leo eine Mail von der Stadtbibliothek: „Bitte heute noch bestätigen.“ Er klickt nicht. Er ruft an.

Irgendwo versucht jemand, sich in eurem Postfach anzumelden. Er kommt nicht hinein.

Ihr habt jetzt weniger Daten und besser geschützte Konten. Und ihr wisst, was ihr im Notfall tut.

Gloria schließt den Schrank auf und legt das Logbuch auf den Tisch. „Noch einmal von vorn“, sagt sie. „Mal sehen, wie weit der Angreifer diesmal kommt.“

2 Schlussrunde 3 Min.

Jede Person sagt einen Satz: Was nehme ich mit? Die Spielleitung als Letzte. Dann tragen alle den Termin für Tag 90 in den Kalender ein, bevor jemand geht.

Die 90 Tage

In der ersten Woche	Die Karte mit ●○○ aus eurem Plan erledigen. Wer fertig ist, sagt es allen.
Nach 30 und 60 Tagen	10 Minuten im Teamtreffen: Was ist erledigt, wo hakt es, wer braucht Hilfe?
An Tag 90	Noch einmal spielen, in 60 Minuten: neuer Check, dann nur die Auflösungen der 6 Runden. Den neuen Schaden im Logbuch neben den alten schreiben.