„Um den Faktor 100 schneller“

Weitreichende Hackerangriffe wie jene im Oktober werden sich häufen. Cybersecurity-Experte Edgar Weippl erklärt, wie Privatpersonen und Organisationen sich schützen.

Das Gespräch führte
Magdalena Schwarz

Eine Viertelstunde benötigt ein KI-versierter Hacker, um Daten zu stehlen. Vor einigen Jahren dauerte das noch Stunden oder Tage. Die PHP-Sicherheitslücken und der Milliardenhack der Kryptobörse Binance zeigen, wie KI den Wettlauf zwischen Cyberkriminellen und Datenschützern anheizt. Wer am Ende gewinnt, kann Edgar Weippl, Professor für Sicherheit und Datenschutz an der Universität Wien, nicht vorhersagen. Bis dahin rät der Leiter der Forschungsgruppe Security & Privacy und Manager beim Forschungszentrum SBA Research zu Sicherheitsmaßnahmen, die erstaunlich „retro“ klingen.

DIE FURCHE: *Für Ihren Beruf müssen Sie denken wie ein Krimineller, das haben Sie 2018 in einem Interview gesagt. Meine Frage heute: Wie denken Kriminelle in Zeiten von Künstlicher Intelligenz?*

Edgar Weippl: Was sich am meisten verändert hat, ist die Geschwindigkeit. Die KI ist ein extrem hilfreiches Tool. Sie erleichtert die Arbeit von Forschenden, die Sicherheitslücken aufspüren und schließen, aber auch von Kriminellen. Dieses Wettrennen hat sich beschleunigt. Der PHP-Vorfall Mitte Oktober hat das verdeutlicht.

DIE FURCHE: *Sie sprechen vom 21. Oktober, als plötzlich viele Websites nicht mehr aufgerufen werden konnten. Was ist passiert?*
Weippl: Zwei Sicherheitslücken in der Programmiersprache PHP wurden online veröffentlicht. Ab dem Zeitpunkt versuchten Websitebetreiber, die Schwachstellen zu schließen, während Angreifer Software entwickelten, um die Lücken auszunutzen. Sind die Hacker schneller, dann können sie PHP-basierte Websites manipulieren, auf sensible Daten zugreifen oder Schadsoftware installieren. Das Problem: Dank KI brauchen Angreifer nur mehr eine Viertelstunde, vor ein bis zwei Jahren hätten sie noch mehrere Stunden oder Tage benötigt. Deshalb haben einige Betreiber ihre Websites vorsorglich abgeschaltet, um Zeit zu haben, die Lücken zu schließen. Auch die Verteidiger müssen KI verwenden, weil der Mensch allein mit der Geschwindigkeit von Hackern nicht mehr mithalten kann.

DIE FURCHE: *Hacken ist also schneller geworden, aber auch einfacher, richtig? Im September wurden gleichzeitig mehrere südkoreanische Banken gehackt. Die US-amerikanische Cybersecurity-Firma CrowdStrike führt den Angriff auf einen 26-jährigen Angreifer in China zurück. Nachdem er die wertvollen Daten gestohlen hatte, fragte er seine KI: „Wie kann ich das zu Geld machen? Wo kann ich es verkaufen?“ Den genialen Hacker mit der schwarzen Kapuzenjacke habe ich mir ehrlich gesagt anders vorgestellt.*
Weippl: Man kommt heute schneller zu Informationen und braucht eventuell weniger Verständnis, das stimmt. Mit den großen US-amerikanischen KI-Systemen lässt sich eine Bank aber nur schwer hacken, dafür beinhalten diese zu viele Sicherheitsvorkehrungen.

DIE FURCHE: *Das heißt, überspitzt formuliert, wenn ich ChatGPT bitte, sich in eine Bank zu hacken, dann wird sich der Chatbot weigern.*
Weippl: Genau. Das Problem sind offenere Modelle, üblicherweise aus China, die jemand mithilfe eigener Hardware selbst betreiben kann, ohne Sicherheitsmechanismen. Damit haben vorwiegend Cyberkriminelle, die etwas vom Hacken verstehen, viel mehr Möglichkeiten, weil sie geschätzt um den Faktor hundert schneller Code generieren, Schwachstellen finden und Angriffe starten können. Denken Sie daran, wie viel schneller Sie dabei sind, einen englischen Text mit KI übersetzen zu lassen und danach das Ergebnis zu kontrollieren, verglichen mit einer manuellen Übersetzung.

DIE FURCHE: *Ende September verschafften sich Hacker Zugriff auf 26.000 interne Dokumente und Daten von 6000 Personen der Stadt Wien. Anfang Oktober wurden bei einem Cyberangriff auf die Universität München 600.000 Datensätze von Studierenden gestohlen. Mitte Oktober haben Hacker aus der Ferne das Abtauen von Kühlanlagen einer französischen Supermarktkette ausgelöst. Mich, als Laiin, beunruhigt das. Wie beunruhigt sind Sie?*
Weippl: Die starke Beschleunigung in so kurzer Zeit ist auf jeden Fall ungewöhnlich. Aktuell gibt es zwei Hypothesen: Die einen sagen, es ist gut, dass KI-Tools gerade viele Schwachstellen aufdecken. Zwei bis drei Jahre lang wird es häufiger Angriffe geben oder Websites werden vorsorglich offline sein, aber danach wird das Internet ein viel sicherer Ort sein. Die anderen prognostizieren, dass parallel auch die KI besser wird, was die Angriffe beschleunigt und weniger nachvollziehbar macht, und dass dadurch alles schlimmer wird. Für mich klingen beide Hypothesen plausibel. Niemand weiß, wie es sich entwickeln wird.

DIE FURCHE: *Sie sind also Agnostiker in dieser Frage?*
Weippl: Wir können die Zukunft nicht vorhersagen. Viel entscheidender ist: Was tun wir jetzt? Ich rate Organisationen zu Risikoanalysen. Welche digitalen Dienste brauche ich stündlich oder täglich, und auf welche kann ich auch für ein paar Tage verzichten? Bei Ersteren lohnt es sich, Back-up-Prozesse einzurichten, für extreme Fälle auch analoge Rückfallmechanismen. Eine Bank muss Wertpapieraufträge vielleicht sofort

bearbeiten, dort lohnt sich die Einrichtung eines Prozesses per Telefon oder Papier. Die Universität Wien dagegen hat beim PHP-Vorfall schlauerweise sofort Websites offline genommen, um potenziell größere Schäden zu verhindern, und deshalb konnte man einen Tag lang nicht auf Onlinekurse zugreifen – das war verkraftbar.

DIE FURCHE: *Schon spannend, dass ein Weg, sich gegen moderne KI-Angriffe zu wehren, die Überlegung ist: Wie hätten wir das vor 20 Jahren gemacht?*
Weippl: Es geht darum, Risiken abzuwägen. Für die kommenden Jahre müssen wir uns darauf einstellen, dass wir immer wieder temporär auf bestimmte Webdienste – Onlinebanking, Webshops, Software für Videocalls, Cloud-Server – nicht zugreifen können werden.

DIE FURCHE: *Sie haben beschrieben, dass sich Organisationen durch Risikoanalysen darauf vorbereiten können. Was raten Sie Privatpersonen? Wir sind schließlich so daran gewöhnt, online zu bezahlen, einzukaufen, zu kommunizieren.*
Weippl: Auch für Privatpersonen sind Risikoanalysen sinnvoll: Wie schlimm ist es für mich, wenn ein bestimmter Dienst kurzzeitig nicht zur Verfügung steht? Wenn zum Beispiel eine App, die ich brauche, um mein Elektroauto zu laden, offline geht, wo kann ich mein Auto dann laden? Für den Fall, dass meine Bank-App nicht funktioniert, habe ich genügend Bargeld zu Hause? Wie viel kostet es, Ersatzlösungen zu etablieren, und ist es mir die Kosten wert?

DIE FURCHE: *Vor einigen Jahren haben wir Menschen noch belächelt, die zu viel Bargeld zu Hause haben oder ihre Überweisungen mit Erlagschein machen. Diese Leute fühlen sich gerade bestätigt. Haben wir die Digitalisierung zu rasch vorangetrieben?*
Weippl: Ein wichtiger Begriff ist die Konvergenz der Dienste: Vor 25 Jahren gab es ein getrenntes Telefonsystem, das heißt, das Festnetztelefon hatte eine eigene Stromversorgung. Selbst bei einem kompletten Stromausfall konnte das Telefonnetz über große, vom Stromnetz unabhängige Batterien aufrechterhalten werden. Mittlerweile läuft unsere gesamte Sprachkommunikation über dieselben Leitungen wie der Internetverkehr. Dadurch ist alles effizienter, schneller und billiger geworden, auch Personal wurde reduziert. Fällt die Automatisierung aber aus, dann ist niemand da, der das System manuell bedienen kann. Durch die Debatte über mögliche Blackouts ist uns diese Abhängigkeit bewusster geworden. Deshalb müssen wir rekonstruieren, was wir alles brauchen, damit ein System ohne Strom funktioniert. Das ist aber nicht so einfach. Denken Sie an eine Tankstelle: Das Pumpen des Treibstoffs passiert maschinell, auch das Abrechnungssystem ist an das Internet angeschlossen, die Rechnungssoftware ist vermutlich cloudbasiert. Allein um Benzin in mein Auto zu füllen, sind zahlreiche Webdienste notwendig. Das zu durchschauen, wird immer schwieriger.

DIE FURCHE: *Ich verstehe jetzt auch besser, was Sie damit meinen, dass Sie wie ein Krimineller denken müssen. Sowohl die Unternehmen als auch die Hacker überlegen, an welchen Stellen es mögliche Sicherheitslücken geben könnte und welche Teilsysteme lahmgelegt werden könnten.*
Weippl: Angreifer und Angreiferinnen versuchen, Bedingungen herbeizuführen, bei denen zwei oder drei Sachen gleichzeitig passieren, die dann ein System zu Fall bringen. Wenn ich eine Stromleitung in Österreich kappe, gibt es Ersatz. Also überlege ich: Welche drei oder vier Leitungen muss ich zerstören, um maximalen Schaden anzurichten?

DIE FURCHE: *Hacker und Hackerinnen sind aber im Vorteil, oder? Zerstören ist einfacher als beschützen. Wenn ich die IT-Leiterin eines Unternehmens bin, muss ich Gesetze und interne Regeln beachten. Ich darf nicht einfach beliebige KI-Software nutzen, um Angriffe abzuwehren. Angreifer sind deutlich flexibler.*
Weippl: Diese Asymmetrie besteht immer zwischen Angreifern und Verteidigern. Ein Einbrecher sucht sich ein Geschäft aus, in das er einbricht; die Polizei muss darauf vorbereitet sein, überall spontan zu reagieren – und sie muss sich dabei an Gesetze halten, die Kriminelle ignorieren können. Umso wichtiger ist es, dass Unternehmen Entscheidungswege verkürzen und IT-Leitungen mehr Autonomie geben. Kleinere und mittelgroße Unternehmen verwenden vermutlich Dienste von großen Betreibern – etwa Microsoft Teams. Diese kümmern sich in der Regel um die Sicherheit ihrer Kundschaft. Man sollte sich trotzdem überlegen, wie man kurzfristig ohne diese Dienste auskommen würde. Für die FURCHE als Wochenzeitung bedeutet das: Können Sie auch eine Ausgabe produzieren, wenn Microsoft zwei Tage nicht zur Verfügung steht? Geht die Welt unter, wenn einmal eine Woche keine FURCHE erscheinen kann?

DIE FURCHE: *Schon, ja. (lacht)*
Weippl: Das stimmt! *(lacht)* Schauen Sie also, dass Sie auch im Ernstfall auf alle Dokumente Zugriff haben und diese nicht ausschließlich in der Cloud liegen.

DIE FURCHE: *Sie haben gesagt, auch Privatpersonen sollten überlegen, welche wichtigen Webdienste sie brauchen und wie sie diese im Notfall ersetzen. Welche Maßnahmen kann ich sonst noch treffen, neben dem altbekannten Tipp, nicht „1234“ als Passwort zu nutzen und Zwei-Faktor-Authentifizierung einzurichten. Wie sollte ich mein Verhalten im digitalen Raum anpassen?*
Weippl: Wir haben mit der Arbeiterkammer Schulungen entwickelt, die zeigen, wie man Fake-Webshops von seriösen Anbietern unterscheidet und andere Betrugsfallen erkennt. Zum Beispiel sollte man kontrollieren, ob eine physische Geschäftsadresse angegeben ist, und bei Google Street View nachsehen, ob es diese Adresse tatsächlich gibt. Natürlich sollte man für jeden Webdienst ein eigenes Passwort nutzen. Auch Betrugsmaschen haben sich durch KI enorm verbessert. Nur weil ich glaube, mit meiner Tante zu telefonieren oder einen Videocall zu führen, muss das nicht meine Tante sein. Deshalb könnten sich Familien ein gemeinsames Codewort überlegen, um die Echtheit des Gegenübers zu verifizieren.

DIE FURCHE: *Spannend!*
Weippl: Prinzipiell ist es auch nützlich, Daten in einer Cloud zu speichern, aber ich würde zusätzlich lokale Back-ups einrichten. Das heißt, digitale Dokumente oder Fotos, die ich nicht verlieren möchte, speichere ich auf einer externen Festplatte oder auf DVDs.

DIE FURCHE: *Wenn ich das alles höre, muss ich Sie noch einmal fragen: Wieso ist es nicht möglich, die Uhr auf eine Prä-Internet-Zeit zurückzudrehen?*
Weippl: Es funktioniert grundsätzlich nicht, technischen Fortschritt zurückzuschrauben. In Österreich gibt es fast täglich Tote durch den Autoverkehr, das Auto lassen wir uns trotzdem nicht nehmen.

DIE FURCHE: *Die einzige Lösung ist also, dass die „Guten“ besser und schneller sind als die „Bösen“?*
Weippl: Es schadet nie, sich zu überlegen, wie man im Notfall agieren würde. Auch Naturkatastrophen werden nicht seltener werden. Wenn ein Tal weggeschwemmt wird, funktioniert vielleicht auch das Onlinebanking für ein paar Tage nicht. Was spricht dagegen, wichtige Dokumente nicht nur digital, sondern zusätzlich auch ausgedruckt in einem Ordner zu lagern? Für rund 150 Euro jährlich bekommt man ein Bankschließfach, in dem man Kopien der wichtigsten Dinge aufbewahren kann. Das hilft nicht nur bei digitalen Ausfällen, sondern auch, wenn das Haus abbrennt. Es ist einfach klug, vorbereitet zu sein.

„Um den Faktor 100 schneller“

A) Vor dem Lesen

a) Erstellen Sie eine Liste aller digitalen Dienste, die Sie gestern genutzt haben (Apps, Plattformen, Online-Banken etc.). Unterstreichen Sie jene Dienste, auf die Sie keinen einzigen Tag verzichten könnten. Vergleichen Sie Ihre Liste mit Ihrer Sitznachbarin bzw. Ihrem Sitznachbarn.

b) Wie stellen Sie sich einen typischen Hacker oder eine typische Hackerin vor? Beschreiben Sie die Person in drei Stichworten.

c) Schätzen Sie: Wie lange braucht ein KI-versierter Hacker heutzutage, um eine Sicherheitslücke auszunutzen und an sensible Daten zu gelangen? Notieren Sie Ihre Schätzung, bevor Sie den Artikel lesen.

B) Textbearbeitung

a) Lesen Sie das Interview mit dem Cybersecurity-Experten Edgar Weippl aufmerksam durch.

b) Vergleichen Sie Ihr Hacker-Bild aus Aufgabe A) b) sowie Ihre Schätzung aus Aufgabe A) c) mit den Informationen aus dem Interview.

c) Erklären Sie folgende Schlagwörter aus dem Interview:

Schlagwort	Erklärung
Sicherheitslücke	
Zwei-Faktor-Authentifizierung	
Konvergenz digitaler Dienste	
Asymmetrie zwischen Angreifern und Verteidigern	
analoger Rückfallmechanismus	

d) Beantworten Sie folgende Fragen zum Text:

- Welche beiden möglichen Zukunftsszenarien in Bezug auf die Entwicklung von Cyberangriffen werden im Interview beschrieben?
- Warum bezeichnet die Interviewerin Edgar Weippl als „Agnostiker in dieser Frage“?

e) Sammeln Sie alle Schutzmaßnahmen, die der Experte Privatpersonen empfiehlt, und ordnen Sie sie in eine Tabelle mit den Spalten „digital“ und „analog“ ein.



C) Textproduktion

Schreiben Sie eine Zusammenfassung.

Lesen Sie das Interview „Um den Faktor 100 schneller", das von Magdalena Schwarz mit Cybersecurity-Experten Edgar Weippl für die Ausgabe der Wochenzeitung „Die Furche" vom 5. November 2026 geführt wurde.

Schreiben Sie nun die **Zusammenfassung** und bearbeiten Sie dabei die folgenden Arbeitsaufträge:

- Geben Sie wieder, wie sich Cyberangriffe durch künstliche Intelligenz verändert haben und machen Sie diese Entwicklung an im Text genannten Beispielen fest.
- Beschreiben Sie die beiden denkbaren Zukunftsszenarien in Bezug auf die weitere Entwicklung von Cyberangriffen, die im Interview erwähnt werden.
- Nennen Sie die digitalen und analogen Schutzmaßnahmen, die der Experte Edgar Weippl Privatpersonen und Unternehmen empfiehlt.

Schreiben Sie zwischen 270 und 330 Wörter. Markieren Sie Absätze mittels Leerzeilen.



D) Weiterführende Aufgaben

Führen Sie in Kleingruppen eine Risikoanalyse durch, wie Weippl sie Organisationen empfiehlt: Welche digitalen Dienste verwendet Ihre Schule täglich (z. B. Stundenplan-App, Lernplattform, E-Mail)? Was passiert, wenn sie eine Woche ausfallen? Entwickeln Sie für jeden digitalen Dienst eine analoge Notfall-Alternative.

Lösungen

Schlagwort	Erklärung
Sicherheitslücke	Fehler bzw. Schwachstelle in einer Software, über die Angreifer Websites manipulieren, auf sensible Daten zugreifen oder Schadsoftware installieren können
Zwei-Faktor-Authentifizierung	Anmeldeverfahren, bei dem zusätzlich zum Passwort ein zweiter, unabhängiger Nachweis nötig ist (z. B. ein Code per App oder SMS)
Konvergenz digitaler Dienste	Früher getrennte Systeme laufen über dieselbe Infrastruktur: Das Festnetz hatte eine eigene Stromversorgung, heute läuft die Sprachkommunikation über dieselben Leitungen wie das Internet. Das ist effizienter und billiger, macht aber abhängig – fällt die Automatisierung aus, kann niemand das System manuell bedienen
Asymmetrie zwischen Angreifern und Verteidigern	Angreifer sind im Vorteil: Zerstören ist einfacher als Schützen. Sie suchen sich ihr Ziel aus und ignorieren Gesetze, während Verteidiger überall vorbereitet sein und sich an Gesetze und interne Regeln halten müssen
analoger Rückfallmechanismus	Nicht-digitale Ersatzlösung für den Notfall, z. B. Wertpapieraufträge per Telefon oder Papier, Bargeld zu Hause oder ausgedruckte Dokumente in einem Ordner

digital	analog
für jeden Webdienst ein eigenes Passwort, nicht „1234“	genügend Bargeld zu Hause, falls die Bank-App ausfällt
Zwei-Faktor-Authentifizierung einrichten	wichtige Dokumente zusätzlich ausgedruckt in einem Ordner lagern
Fake-Webshops erkennen: physische Geschäftsadresse prüfen und bei Google Street View kontrollieren	Kopien der wichtigsten Dinge in einem Bankschließfach (ca. 150 Euro jährlich) aufbewahren
Daten in der Cloud und zusätzlich lokal sichern (externe Festplatte, DVDs)	gemeinsames Familien-Codewort, um die Echtheit des Gegenübers am Telefon oder im Videocall zu prüfen
persönliche Risikoanalyse: Welche Dienste brauche ich wirklich?	Ersatzlösungen überlegen (z. B. wo man das E-Auto lädt, wenn die App offline ist) und durchdenken, wie man im Notfall handeln würde