Interview mit Calvin Hollywood

Hey Leute, was geht ab? Hier ist Calvin. Herzlich Willkommen zu einer weiteren Podcastfolge. Das ist mit Abstand die spontanste Podcastfolge, die ich je gemacht habe. Ich war eigentlich bei einem Fotoshooting und habe jetzt jemanden kennengelernt, bei dem ich dachte: „Hey, du musst in meinen Podcast." Ich habe jetzt einfach die Kamera aufgestellt, nicht für ein Video, aber um den Ton damit aufzunehmen. Also wundert euch bitte nicht, wenn der Ton nicht perfekt ist, aber ich wollte René einfach hier direkt in die Podcast-Show holen.

Ganz kurzes Intro: René hat mich als Fotograf gebucht um Bilder für seine Website, für Social Media Auftritte, usw. zu machen. Er erklärt euch gleich selbst nochmal, was er macht. Wir haben so tolle und spannende Gespräche geführt, dass einfach klar war, dass er in den Podcast muss.

C: „René, erstmal schön, dass du da bist."
R.: „Ich danke dir für die Einladung, Calvin."

C.:" Ja, sehr gerne. Also René, jetzt erzähl mal: was machst du, wer bist du und woher kommst du?"
R.: „Ich bin René Hippen, ich komme aus Minden, bin 26 Jahre alt und bin Speaker und im Bereich Coaching mit dem Schwerpunkt Internetsicherheit unterwegs."

C.: „Sehr cooles Thema. Also du bist derjenige, der Firmen oder Leute im Bereich Internetsicherheit berät, so dass sie nicht von außen gehackt werden können."
R.: „Genauso schaut's aus."

C.: „Jetzt weiß ich nicht, wie tiefgründig wir da reingehen können. Wir lassen den Punkt mal fast aus, aber charmant formuliert: Du kennst beide Seiten. Einmal weißt du, wie man Leute im Internet vor Hacking beschützt, zum anderen aber auch, wie Hacker arbeiten. Und daher weißt du, wie solche Leute ticken."
R.: „So ist es. Ich kenne beide Seiten. Ich war auch auf der dunklen Seite lange genug aktiv. Aus dieser Zeit weiß ich genau, wie ich Unternehmen und Privatpersonen schützen kann."

C.: "Okay, aber das darf man jetzt auch so sagen, oder? Nicht, dass hier gleich die Polizei kommt und dich mitnimmt."
R.: „Nein, nein, keine Angst. Da war ich minderjährig."

C.: „Vor allen Dingen hast du einfach Ahnung von der Materie. Wir haben uns ja eben schon länger unterhalten. Ich habe mal den Film „How am I" gesehen. Das ist ein sehr spannender Film über's Hacken. Da wird die Szene ja ziemlich cool dargestellt. Es ist der Wahnsinn, was man da alles machen kann. Gib der Community doch mal drei Tipps – und wir fangen da wirklich mal mit den Basics an – wie man sicherer im Internet unterwegs ist. Wenn da noch weiteres Interesse besteht, können wir

später nochmal ein Skype-Interview machen, wo wir ein bisschen tiefgründiger reingehen. Und lass uns mal mit dem Punkt Drei anfangen, den wir eben schon kurz vorbereitet haben. Thema Passwörter. Ich nutze die App ‚Passwords' um meine Passwörter zu speichern. Was hältst du von solchen Apps, die Passwörter sammeln? Was gibt es da bei der Nutzung zu beachten?"
R.: „Erstmal sind sie gar nicht schlecht. Ganz wichtig ist es aber darauf zu achten, wo die Passwörter gespeichert werden. Werden sie in einer Cloud bei einem Drittanbieter irgendwo auf der Welt gespeichert? Das würde bedeuten, dass ich meine wichtigen Passwörter irgendjemandem anvertraue und gar weiß nicht, was damit passiert. Darum bin ich ein Befürworter der App ‚1Password'.

C.: „Was ist an ‚1Password' anders?
R.: ‚1Password' ist für alle Betriebssysteme nutzbar und man kann die Passwörter in einen sogenannten Container legen, der auf deinem Rechner oder auf einem USB-Stick gespeichert ist. Das heißt also, du hast deine Passwörter immer bei dir und musst die nicht aus der Hand geben."

C.: „Ah okay, check! Das ist ja wichtig!"
R.: „Genau so sieht es aus. Man speichert da ja wichtige Daten drin, wie zum Beispiel Passwörter fürs Banking. Und die sollten sicher aufgehoben sein."

C.: „Ist es denn so, dass man sich auf Hackerseite sehr auf diese Tools stürzt, weil da sehr viele Passwörter zu holen sind? Okay, er nickt schon."
R.: „Ja, exakt so ist das."

C.: „Wäre es jetzt also angebracht, bei meiner App mal zu checken, wo die Daten gespeichert werden? Das kann man ja bestimmt rausbekommen."
R.: „Klar, das wäre der erste Schritt zu mehr Sicherheit."

C.: „Wenn sie also in der Cloud liegen, würdest du eher einen anderen Dienst empfehlen, weil das Backup auf jeden Fall auf dem Rechner oder einem USB-Stick hinterlegt sein sollte."
R.: „Richtig. Wenn ich an dem Punkt zu ‚1Password' noch was sagen darf: man kann die App so einstellen, dass beispielsweise bei einem Apple-Gerät alles in der iCloud gespeichert wird oder es gibt die Möglichkeit, die Daten automatisch auf einem USB-Stick oder auf dem Rechner zu speichern. Besonders praktisch ist dann, dass sich die Passwörter mit dem Smartphone oder mit einem anderen Rechner synchronisieren. Aber nur – und das ist sehr wichtig – wenn sie in einem gemeinsamen WLAN eingeloggt sind und man gleichzeitig eine sichere Verbindung hat."

C.: „Okay, dann vielleicht nochmal kurz was zu Thema Passwort selbst. Auch wenn das ein eigentlich einfacher Tipp ist. Es verwenden ja bestimmt viele immer noch ‚Test1234' oder etwas ähnlich einfaches als Passwort. Gibt es da Regeln, die man bei der Erstellung eines Passworts beachten sollte, um es Hackern so schwer wie möglich zu machen?

René Hippen
Lemgoer Str. 65
31737 Rinteln

Mail: moin@renehippen.de
Telefon: 0800 50 64 202

R.: „Auf jeden Fall sollte man auf die Länge des Passwortes achten. Es muss mindestens acht Zeichen haben, besser ist es, noch mehr zu verwenden. Dann ist es natürlich auch wichtig, die Variation innerhalb des Passworts zu beachten. Es sollten Sonderzeichen, Kleinbuchstaben, Großbuchstaben und Zahlen enthalten sein und es ganz wichtig ist auch, dass es kein Wort ist, was im Duden zu finden ist."

C.: „Ach so! Okay."
R.: „Alle Wörter, die im Duden stehen, werden zum Knacken von Passwörtern direkt als Erstes ausprobiert."

C.: „Gibt es dafür Programme, die den ganzen Duden einmal durchtesten oder wie funktioniert das?"
R.: „Ja, so ist es. Es gibt Programme, die einfach die Standardpasswörter durchgehen. Und sowas gibt es auch in Form einer sogenannten ‚Dictionary Attack'. Das heißt, dass Dateien mit dem kompletten Inhalt des deutschen Dudens durchlaufen, ob da das gesuchte Passwort dabei ist."

C.: „Das heißt zusammengefasst: Passwort gut überlegen, die verschiedenen Möglichkeiten, die die Zeichen bieten, auch nutzen und lange Passwörter verwenden. Außerdem sollte man ‚1Password' benutzen oder bei einer anderen App dementsprechend aufpassen, wo die Daten konkret gesichert werden. Ich weiß, dass viele jetzt vielleicht denken, dass diese Punkte total selbstverständlich sind. Aber das Problem ist leider oft, dass es das eben nicht ist, oder?"
R.: „Nein, die überwiegende Mehrheit beachtet diese Tipps leider bis jetzt nicht."

C.: „Genau, es gibt genügend Leute – und da zähle ich mich selbst auch dazu – die die Sicherheit im Internet etwas sportlicher nehmen. Da muss meistens erstmal was passieren, bevor man da reagiert. Okay, gehen wir mal zum zweiten Thema: die Cloud. Die Cloud hat ja großes Potential für die Zukunft. Jetzt gibt es ja viele verschiedene Anbieter. Du hast vorhin gesagt, du empfiehlst eher eine eigene Cloud, oder?"
R.: „Für für den normalen Privatanwender, der nur seine Bilder hochlädt und von unterwegs ab und zu darauf zugreifen möchte, ist eine private Cloud einfach günstiger. Da hat man keine monatlichen Kosten und die Daten liegen ganz sicher."

C.: „Das ist also für Leute geeignet, die sich einfach nicht so gut mit Datensicherheit auskennen. Das heißt, du kaufst dir ein Gerät und stellst das irgendwo im Unternehmen oder zu Hause ab. Übers Internet kannst du dann von überall aus darauf zugreifen und alle deine Daten darauf speichern und abrufen."
R.: „Genau. Das ist wirklich kinderleicht einzurichten mit einer Step-by-Step Anleitung, die in den meisten Fällen mitgeliefert wird oder sonst online zu finden ist."

C.: „Cool, Okay. Jetzt mal ganz kurz zum Thema Dropbox. Das ist ja auch eine Cloud, die sehr viele Privatanwender nutzen. Was hältst du von Dropbox?"

René Hippen
Lemgoer Str. 65
31737 Rinteln

Mail: moin@renehippen.de
Telefon: 0800 50 64 202

R.: „Ich bin kein großer Fan von Dropbox. Schon alleine, weil die rechtliche Seite da für Unternehmen problematisch ist. Privatanwender können sie gerne nutzen, aber man sollte möglichst keine vertraulichen Daten darauf speichern. Bilder sind in Ordnung. Unternehmen müssen sich aber in Deutschland an das Datenschutzgesetz halten. Darin ist festgelegt, was für einen Sicherheitsstandard ein Cloudanbieter haben muss. Da Dropbox den Firmensitz nicht in Deutschland hat, müssen sie sich aber nicht an deutsches bzw. europäisches Recht halten. Das kann für Unternehmen zum Problem werden."

C.: „Oh ha! Das wissen aber wahrscheinlich viele auch nicht."
R.: „Genau. Da passieren ganz schnell unwissentlich Gesetzesverstöße. Darum sollte man sich, wenn man die Cloud wirklich kommerziell nutzen möchte, irgendwo in Deutschland oder im EU-Bereich einen Cloud-Anbieter suchen."

C.: „Welchen kannst du da empfehlen?"
R.: „Wer da nicht viel investieren, aber hohe Sicherheitsstandards möchte, der ist als kleines Unternehmen bei ‚Strato' gut aufgehoben. Für größere Unternehmen gibt es dann zum Beispiel ‚Center Device'."

C.: „Und auch hier ist wahrscheinlich wieder wichtig zu schauen, wo die Anbieter ihren Firmensitz haben.
R.: „Genauso ist es. Sie müssen den gesetzlichen Bestimmungen gerecht werden."

C.: „Jetzt hast du gesagt: ‚Keine wichtigen Daten in die Dropbox'. Gibt es da noch irgendeinen Tipp? Ich könnte dir doch jetzt zum Beispiel auch Bilder über die Dropbox schicken und sie danach gleich wieder löschen. Dann kommt keiner mehr an die Daten."
R.: „Doch, das geht unter Umständen trotzdem noch. Zum Beispiel vergessen die Meisten, dass gelöschte Bilder bei Dropbox immer erstmal in den Ordner ‚Papierkorb' verschoben werden. Wenn man die Daten da nicht noch einmal extra rauslöscht, können sie innerhalb der nächsten 30 Tage weiterhin abgerufen werden."

C.: „Da könnte man allerdings auch wieder ein Passwort verwenden."
R.: „Genau, aber auch hier wieder darauf achten: immer ein Passwort verwenden, das nicht so leicht zu erraten ist."

C.: „Dann lass uns nochmal zum dritten Thema kommen, über dass wir uns vorhin unterhalten haben. Ich bin ja viel unterwegs in Hotels und an öffentlichen Plätzen und nutze da häufig offene WLANs. Du hast mir da ja schon einige Geschichten erzählt, wie sich Hacker durch solche ungesicherten Netzwerke zu meinem Smartphone oder Laptop Zugang verschaffen können. Was gibt es da zu beachten?"
R.: „Bei offenen WLANs, zum Beispiel bei Hotspots bei der Telekom, sollte man immer darauf achten,

dass man keine vertraulichen Daten versendet oder eingibt. Denn alle, die im gleichen WLAN eingeloggt sind, können mehr oder weniger mitlesen."

C.: „Aber nur, wenn sie sich gut auskennen, so wie du, oder?"
R.: „Genau. Das nennt sich ‚Man in the Middle' , sprich ‚Der Mann in der Mitte'. Wenn jemand weiß, wie es geht, kann er die Daten abfangen. Das heißt also alles, was du vielleicht gerade per E-Mail verschickt hast, kann derjenige in Klartext mitlesen und weiß dann zum Beispiel: ‚Der Mann da drüben an der Bar trifft sich nachher mit seiner Geliebten und seine Frau sitzt zu Hause."

C.: „Wow, Okay. Ich will ja nicht wissen, was du da schon so alles gefunden hast. Okay, dann noch eine Frage. Ich benutze öfter einen Surfstick, um online zu gehen. Sind die auch so unsicher, wie offene WLAN-Hotspots?"
R.: „Nein, die sind einigermaßen sicher. Auf jeden Fall viel sicherer als offene Netze. Du bist ja alleine in diesem Netz, dass deine WLAN-Box erzeugt. Dementsprechend sollte aber auch da das WLAN-Passwort wieder gut gewählt sein."

C.: „Ich habe jetzt bei vielen Geräten, die ich nutze, noch das originale Passwort drin, das vom Hersteller vorgegeben war. Ist das ein No-Go?"
R.: „Das ist ein absolutes No-Go! Das würde ich sofort ändern. Diese Standard-Passwörter sind meistens irgendwo im Netz zu finden. Da braucht man wirklich nur zu wissen, wie man Google nutzt und bekommt sofort die entsprechenden Passwörter geliefert. Darum empfehle ich immer, bei einem neuen Router zum Beispiel, sofort den Namen zu ändern, sodass man nicht mehr rückschließen kann, von welchem Hersteller der Router kommt und natürlich auch das Passwort sofort zu ändern."

C.: „Echt krass. Wir haben jetzt 14 Minuten aufgenommen und da waren schon so gute Infos dabei. Und wir haben bis jetzt nur an der Oberfläche gekratzt."
R.: „Ja, da könnten wir noch deutlich tiefer gehen, aber dann sitzen wir morgen noch hier."

C.: „Stimmt, aber es geht auch nicht immer darum, den Menschen was komplett Neues zu vermitteln. Ich will nicht wissen, wie viele Zuhörer sich gerade denken, dass sie dringend mal wieder ein Passwort ändern müssten, oder das originale Passwort mal ändern sollten, oder den Ort, wo sie ihre Passwörter hinterlegt haben, mal überprüfen müssten. Ich glaube, viele denken: ‚Ach, bisher ist mir noch nie was passiert'. Und wisst ihr, was René dazu sagt? Das denkst du nur. Und damit hat er recht! Du weißt gar nicht, ob du schon angegriffen wurdest. Viele greifen gar nicht unbedingt die einzelne Person an, sondern holen sich Daten, mit denen sie zum Beispiel an Kunden der Person rankommen, um da immer mehr Infos rauszuziehen."
R.: „Genau, da liegt das Problem. 80 Prozent der Angriffe bekommen die Unternehmen gar nicht mit. Und wenn da schon Unternehmen Probleme haben, Angreifer schnell zu identifizieren, wie soll das

dann eine Privatperson merken. Die Leute, die aufdecken, dass Unternehmen angegriffen wurden, sind fast immer Drittanbieter. Die werden dann geholt, wenn es einen Verdacht auf eine Hackerattacke gibt. Das sind dann so Leute wie ich oder auch die Polizei. Und Hacker bleiben auch nicht nur ein oder zwei Tage unbemerkt, sondern oft über mehrere Monate. In dieser Zeit können sie unvorstellbaren Schaden anrichten."

C.: „Okay, das ist wirklich nicht vorstellbar. Was das auch für Kosten sind, die da entstehen. Also Freunde, ich kenne jetzt einen Experten, der mir bei der IT-Sicherheit helfen kann, aber ihr könnt ihn auch selbst kontaktieren. Wir haben jetzt hier mal ein paar Tipps an euch rausgegeben, aber zu guter Letzt: wenn ihr Hilfe in der IT-Sicherheit benötigt, sprecht René an. Er hilft euch gerne. Egal, ob ihr Privatkunden seid oder Unternehmen. Er checkt bei euch durch, wie sicher ihr im Internet aufgestellt seid. Das macht er zum Teil direkt von zu Hause aus. Er deckt eure Lücken auf und kann euch helfen, diese zu beseitigen, so dass ihr euch keine Sorgen mehr um die Sicherheit eurer Daten machen müsst."

R.: „Ich kann hier auch noch ein kleines Angebot machen: alle, die mich über Calvin kontaktieren, die kriegen die ersten 30 Min. über Skype komplett kostenlos als Erstberatung. Ich will, dass jeder einen gewisse Grundsicherheit hat. Das ist meine Mission. Ich möchte, dass jeder weiß, wo sind die Gefahren und wie schütze ich mich.

C.: „Du hast ja auch eine Facebook-Seite. Da könnt ihr René kontaktieren. Du bist Speaker und hast einen YouTube-Kanal und ein eigener Podcast ist in Planung. Da kommt einiges, wo die Leute dir folgen, und sich weiterhin über ihre IT-Sicherheit informieren können. Vielen Dank für deine Zeit René und bis zum nächsten Mal."

R.: „Ich habe zu danken. Ich komme gerne wieder."

René Hippen
Lemgoer Str. 65
31737 Rinteln

Mail: moin@renehippen.de
Telefon: 0800 50 64 202