IT-Sicherheit: Ethisches Hacken

By Joël Adami | 2018-03-22 | Thema

Der Fall „ChamberLeak“ zeigt, dass in Luxemburg wenig Bewusstsein für das Problem vorhanden ist, wie mit Sicherheitslücken umgegangen werden soll.

Die meisten Hacker*innen sind nicht böse – aber sie suchen nach Sicherheitslücken und werden deswegen oft kriminialisiert. (Fotos: CC-BY Hivint)

Am 7. März deckte der öffentlich-rechtliche Radiosender 100,7 eine Sicherheitslücke auf der Website des luxemburgischen Parlaments auf. Was künftig „ChamberLeak“ genannt werden wird, war keine besonders komplizierte Lücke. Es musste kein Passwort erraten und kein Programmiercode ausgeführt werden – es genügte, eine Ziffer in der URL, also der Adresse des gewünschten Dokuments, zu ändern.

Die Affäre zeigt, dass die IT-Sicherheitskultur luxemburgischer Institutionen dringend überprüft werden muss, und sie wirft weitere interessante Fragen auf: Wie soll sich eine Person, die zufällig auf eine Sicherheitslücke stößt, verhalten, was soll sie tun? Welche Regeln gibt es für Sicherheitsforscher*innen, die systematisch nach Schwachstellen suchen? Der Vergleich mit Whistleblower*innen liegt auf der Hand, ist jedoch nicht unbedingt zutreffend. Die Frage, wie Organisationen und Institutionen mit Meldungen zu Sicherheitslücken umgehen, ist sehr wichtig – werden solche Meldungen falsch behandelt, kann das dazu führen, dass Lücken überhaupt nicht mehr gemeldet werden.

Die politisch interessierte Person, die auf die Sicherheitslücke der Parlamentswebseite stieß, lud sich mithilfe eines Programms automatisiert sämtliche verfügbaren PDF-Dokumente von der Website. Da die Dokumente – parlamentarische Anfragen, Gesetzesvorschläge, Stellungnahmen von Staatsrat und Kammern, usw. – alle fortlaufend nummeriert waren, war dies technisch relativ leicht zu realisieren. Ähnlich könnte auch vorgehen, wer sämtliche woxx-Nummern als PDF aus unserem Archiv herunterladen wollte.

Ohne Sicherheitsvorkehrungen kein Eindringen

Auf der Parlamentswebseite fanden sich unter den Dokumenten jedoch auch solche, die nicht für die Öffentlichkeit bestimmt waren. Detaillierte Pläne der Parlamentsgebäude, Berichte der Geheimdienstkommission, Personalakten – und ein Protokoll, aus dem hervorgeht, dass die Parlamentarier*innen der Meinung sind, die Presse interessiere sich nicht genügend für ihre Arbeit.

Obwohl Parlamentspräsident Mars Di Bartolomeo sich gleich nach der Aufdeckung der Lücke bei Radio 100,7 bedankt hatte, schlug die Kommunikationsabteilung der „Chamber“ schnell andere Töne an: Von einem „Eindringen“ oder gar einem „Hack“ war die Rede. In Wirklichkeit war gar kein Eindringen in ein internes System nötig, die Dokumente waren öffentlich abrufbar – wenig überzeugend also, hier von „Eindringen“ zu reden. Am 9. März entschied das Parlamentsbüro, der Zusammenschluss der Fraktionsvorsitzenden, den Fall an die Staatsanwaltschaft weiterzuleiten. Auch die nationale Datenschutzkommission CNPD schaltete sich ein.

Der Begriff „hacken“ ist sehr schwammig – und hat im medialen und umgangssprachlichen Gebrauch eher eine negative Bedeutungsfärbung. Ein „Hack“ kann zum Beispiel auch eine schlechte, unelegante Lösung eines Programmierproblems sein. Dass es sich andererseits bei einem „Hackerspace“, also einem Raum in dem sich an Computer und Technik interessierte Personen zum gemeinsamen Programmieren und Basteln zusammenfinden können, nicht um einen Ort für organisierte IT-Kriminalität handelt, ist auch klar – hier wird versucht, den Begriff wieder positiv zu besetzen.

Wenn man vom „hacken“ oder „eindringen“ in ein Computersystem spricht, kann man davon ausgehen, dass eine Sicherheitsvorkehrung überwunden wurde. Dies war beim „ChamberLeak“ jedoch definitiv nicht der Fall: Die PDF-Dateien waren frei zugänglich, höchstens dadurch „versteckt“, dass es keine öffentlichen Links auf sie gab. Das Parlament muss sich nun die Frage gefallen lassen, warum die Website als interner Dokumentenserver benutzt wurde. Vor allem, nachdem der Fehler, den Radio 100,7 aufgedeckt hat, schon vor Jahren einmal behoben worden war.

Verantwortungsbewusste Hacker*innen

Für Leute, deren Beruf oder Hobby es ist, Sicherheitslücken in den Systemen anderer ausfindig zu machen, gibt es strenge Regeln. Mittlerweile gibt es sogar Lehrgänge für „Ethisches Hacken“. Allerdings wird überwiegend der Begriff „Security Research“, also Sicherheitsforschung, verwendet – durchaus auch, um den Begriff „Hacker*in“ zu rehabilitieren: Die meisten Hacker*innen sind von Neugier und Wissbegierde getrieben, nicht von krimineller Energie. Wer den bezahlten Auftrag bekommt, ein System von Kopf bis Fuß zu durchleuchten, muss sich sowieso an Spielregeln halten und wird die aufgedeckten Daten nicht weitergeben. Menschen, die Sicherheitsforschung in ihrer Freizeit betreiben, bewegen sich manchmal auf recht dünnem Eis. Vor allem dann, wenn sie eine Sicherheitslücke gefunden haben.

„Responsible Disclosure“, also „verantwortungsbewusste Enthüllung“ nennt sich das Prinzip, gemäß dem auf solche Lücken aufmerksam gemacht werden soll. Viele IT-Firmen haben eine spezielle Rubrik auf ihrer Website, in der beschrieben ist, wie ein Fehler gemeldet werden soll. Grundsätzlich gilt, dass der Organisation einige Zeit gelassen werden muss, den Fehler zu beheben, bevor man an die Öffentlichkeit geht. Meistens sind dies 30 Tage, die Frist kann allerdings auch länger sein oder auf Anfrage verlängert werden. Bei Hardware-Fehlern kann es bis zu einem halben Jahr dauern, bis eine Schwachstelle öffentlich gemacht wird. Mit diesem Vorgehen soll verhindert werden, dass Menschen mit schlechten Intentionen Fehler ausnutzen, bevor sie behoben sind.

Wenn die betreffende Organisation (Soft- oder Hardwarehersteller, soziales Netz, öffentliche Einrichtung, usw.) innerhalb der gewährten Periode nicht reagiert, machen die Hacker*innen die Lücken öffentlich. Die betreffende Organisation wird auf diese Weise unter Druck gesetzt, damit sie die Sicherheitslücke umgehend schließt. Spätestens zu diesem Zeitpunkt wird dann auch die Presse informiert. Um sich selbst vor Strafverfolgung zu schützen, agieren Sicherheitsforscher*innen oft anonym bzw. unter einem Pseudonym. Manche Organisationen bieten auch „Kopfgelder“ auf Sicherheitslücken an und behandeln jede Meldung vertraulich – oft versprechen sie auch, keinerlei juristische Schritte einzuleiten. Beim „responsible disclosure“-Modell haben also beide Seiten Rechte und Pflichten.

„Man kann sich an die Betroffenen wenden und ihnen erklären, dass man keinen Schaden angerichtet hat und dies auch nicht beabsichtigt. Wer sich das selbst nicht zutraut, kann zum Beispiel Circl oder GovCert als Mittler einschalten. Auch der C3L hat in solchen Fällen schon vermittelt“, erklärt Sam Grüneisen, der Pressesprecher des luxemburgischen Chaos Computer Clubs (C3L).

Das Circl (Erklärungen im Kasten) hat eine eigene „responsible disclosure“-Seite, auf der im Detail beschrieben wird, wie man vorgehen soll, wenn man eine Sicherheitslücke entdeckt. Für staatliche Institutionen gibt es beim

GovCert bzw. bei der Restena (für das Bildungswesen) ähnliche Meldestellen. Nach einer Meldung von Radio 100,7 arbeitet das Parlament jedoch nicht mit GovCert oder anderen staatlichen Informatikdiensten zusammen – angeblich, um die Gewaltentrennung zu gewährleisten.

Auch wenn das Parlament es sich so vorstellt: So sieht Datenklau eher selten aus.

Sicherheitslücken lieber nicht zuerst an die Presse

„Sich an die Medien zu wenden, ohne jemanden wie Circl, GovCert oder uns um Rat zu fragen, ist keine gute Idee. Das wird meistens als ziemlich aggressive Taktik empfunden und kommt bei den Betroffenen nicht gut an, weil es natürlich keine gute PR ist.“, so C3L-Sprecher Grüneisen. Für Hacker*innen, die in der Szene aktiv sind und das „responsible disclosure“-Konzept kennen, ist dieser Gedankengang sicherlich nachvollziehbar. Für Menschen, die durch Zufall auf eine Sicherheitslücke stoßen, aber eher nicht – für sie sind die Medien wohl doch erste Ansprechpartner. Vor allem dann, wenn sie auf Dokumente gestoßen sind, an denen die Öffentlichkeit ein Interesse haben könnte – wie zum Beispiel eine Budgeterhöhung für den Geheimdienst.

Die Ankündigung des Parlaments, den „ChamberLeak“ strafrechtlich verfolgen zu wollen, ist auf harsche Kritik gestoßen, zum Beispiel vom Journalist*innenverband ALJP. „Auf Grundlage dieser speziellen Ausgangssituation, der prinzipiell mit großer Sorgfalt zu begegnen ist, stellen wir fest, dass es hier offensichtliche Einschüchterungsversuche gegeben hat. Die ALJP steht als Berufsorganisation für die Pressefreiheit ein und toleriert keine Einschüchterungsversuche gegenüber professionellen Journalisten. Die ALJP weist in diesem Kontext darauf hin, dass es in Luxemburg noch keinen umfassenden Schutz für Whistleblower gibt, die im öffentlichen Interesse Missstände aufdecken“, hieß es in einer Pressemitteilung.

Whistleblower*innen agieren meistens aus einer Organisation heraus, während hier einer externen Person zufällig eine Sicherheitslücke aufgefallen war. Das heißt nicht, dass die Forderung nach einem Schutz für Whistleblower*innen hinfällig oder der Einschüchterungsversuch gegenüber Journalist*innen weniger streng zu verurteilen wäre. Denn auch, wenn das Parlament bestreitet, dass die rechtlichen Schritte auf Einschüchterung abzielen – dass sie einen gewissen „chilling effect“ haben, ist nicht zu leugnen. Dennoch stellt sich die Frage, ob ein Whistleblower*innenschutz in diesem Fall überhaupt gegriffen hätte.

Whisteblower*innen und Kopfgeld

Der Staat solle sich glücklich schätzen, dass überhaupt irgendwer etwas meldet, und nicht gleich mit Strafanzeigen reagieren, meint auch der C3L. „Das Verhalten trägt dazu bei, dass Sicherheitslücken nicht gemeldet oder gar weiterverkauft werden. Man müsste auch den Weg gehen, ein Bug-Bounty-System einzuführen, also Belohnungen für aufgedeckte Fehler anzubieten“, so Grüneisen. Vor dem Hintergrund, dass laut eines 100,7-Berichts eine Sicherheitslücke nicht gemeldet wurde, weil GovCert keine Straflosigkeit zusichern wollte, eine verständliche Forderung. Die Passwörter von über 1.000 Personen, darunter Politiker*innen und Journalist*innen, sollen im Klartext auslesbar gewesen sein. Eine offizielle Stellungnahme dazu steht noch aus, die CSV hat bereits eine parlamentarische Anfrage zu dem Thema gestellt.

Beispiele für einen positiven Umgang mit Entdecker*innen von Sicherheitslücken gibt es in Luxemburg jedoch auch: „Uns sind Fälle von Menschen, die eine Belohnung bekommen haben, bekannt. Das läuft in Luxemburg aber alles unter der Hand. Oft wissen die Firmen jedoch nicht, was genau passiert ist und setzen eher auf strafrechtliche Verfolgung. Wir würden uns einen klaren gesetzlichen Rahmen und mehr Sensibilisierung zu der Thematik wünschen.“

Luxemburg möchte sich als IT-Standort positionieren. Die Website des Parlaments mag ein Sonderfall sein – der Umgang mit Personen, die Sicherheitslücken finden, ist es jedoch nicht. Es wäre also definitiv wünschenswert,

dass sich die Abgeordneten demnächst mit dem Thema „responsible disclosure“ beschäftigen – am Besten nicht nur im Hinblick auf ihre eigene Website.

IT-Sicherheit in Luxemburg

Smile: „Security made in Luxembourg“ nennt sich das staatliche Zentrum, das sich für IT-Sicherheit in der Privatwirtschaft und beim Staat einsetzt. Mehrere Initiativen in dem Bereich gehen von Smile aus.
Circl: Das „Computer Incident Response Center“ ist sozusagen die Feuerwehr des Internets. Neben Trainings für den Fall der Fälle kann die Organisation bei einer Cyberattacke oder dem Bekanntwerden einer Schwachstelle unverzüglich eingreifen.
Cases: Die „Cyberworld Awareness and Security Enhancement Services“ bieten Informationen und Dienstleistungen für die Privatwirtschaft an. Ziel ist es, die Sicherheit der IT-Infrastruktur zu stärken.
*C3: Das „Cybersecurity Competence Center“ ist ebenfalls eine Initiative von Smile und bietet Kurse für IT-Sicherheitsexpert*innen an.*
*Bee Secure: Die Initiative, die vom Wirtschafts- und Familienministerium getragen wird, informiert „normale“ Bürger*innen über IT-Sicherheit. Im Blick sind hierbei vor allem Kinder, Jugendliche sowie Eltern und Betreuer*innen.*
GovCert: Cert steht für „Computer Emergency Response Team“, das GovCert ist jene Organisation, die für die IT-Sicherheit der meisten staatlichen Organisationen verantwortlich ist. Für die IT-Infrastruktur des Bildungswesens ist zum Beispiel der seperate Dienst Restena bzw. das „Restena-Csirt“ zuständig.
*C3L: Der Chaos Computer Club Luxemburg ist ein Verein von Hacker*innen und anderen IT-Interessierten, der sich für Informationsfreiheit und Datenschutz einsetzt.*

Tagged woxx1468.