BUG BOUNTY SWITZERLAND

USZ Universitäts Spital Zürich

CASE STUDY

Informationssicherheit & Bug Bounty in Spitälern

Erhöhtes Risiko für Cyberangriffe in der Gesundheitsbranche

Die Gesundheitsbranche ist aufgrund der digitalen Transformation laufend neuen Herausforderungen ausgesetzt. Spitäler, Labore und andere Gesundheitseinrichtungen haben viele Prozesse wie zum Beispiel die Verwaltung von Patientendaten, oder auch die Messung von Gesundheitsdaten wie Blutdruck und Herzraten digitalisiert. Diese Daten gilt es nun vor böswilligen Attacken und unberechtigten Zugriffen zu schützen. Insbesondere seit dem Beginn der Corona-Pandemie ist ein Anstieg der gezielten Angriffe auf Gesundheitseinrichtungen zu verzeichnen. So haben gezielte Cyberattacken auf Spitäler und andere Gesundheitseinrichtungen signifikant zugenommen.

«Spitäler werden immer mehr digital und sind hochgradig ins Netz integriert. So gibt es auch immer mehr Webbased Applications wie beispielsweise das Patientendossier. Falls die IT-Struktur ausfällt, ist das Spital ausser Gefecht gesetzt. Der Erfolg des Spitals steht und fällt somit mit der Informationssicherheit.»

Erik Dinkel *M.A. Chief Information Security Officer (CISO) des Universitätsspitals Zürich*

Hohes Angriffsniveau bei Spitälern gefährdet die Sicherheit der Patientinnen und Patienten

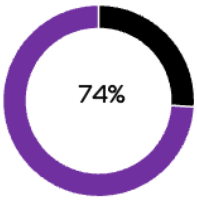
Insbesondere Spitäler sorgen sich, nicht nur um den Verlust vertraulicher Patienten- und Unternehmensdaten, sondern auch um die Sicherheit der Patientinnen und Patienten. Erik Dinkel, CISO des Universitätsspitals Zürich meint hierzu: „Bei einem erfolgreichen Cyber Angriff sind nicht nur finanzielle Schäden im mehrstelligen Millionen Bereich möglich, sondern auch mit Auswirkungen auf den Spitalbetrieb und möglichen negativen Folgen für die Patientinnen und Patienten zu rechnen. Die Schliessung von Abteilungen, wie Notaufnahmen und Intensivstationen, kann dazu führen, dass Patientinnen und Patienten abgewiesen werden müssen oder nicht weiter behandelt werden können. So kann es zu lebensbedrohenden Situationen kommen.“ Spitäler, welche angegriffen werden, haben deshalb eine hohe Bereitschaft die Lösegeldforderungen zu zahlen. Wie das hohe Angriffsniveau während der Covid-19 Pandemie zeigt, nutzen Cyber Kriminelle dies aus und greifen vermehrt und gezielt Gesundheitseinrichtungen an.

«Wir haben sehr schützenswerte Daten von Patientinnen und Patienten sowie höchste Anforderungen an die Verfügbarkeit unserer Systeme. Dies gilt es zu schützen und ein sicheres Umfeld zu schaffen. Wir müssen alles tun, um die Datensicherheit und die Verfügbarkeit der Systeme sicherzustellen.»

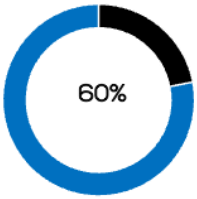
Fabian Kälin *Analyst Security Operating Center des Universitätsspitals Zürich*

Das Schweizer Gesundheitswesen muss vor Cyber-Angriffen geschützt werden

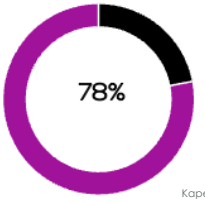
Wie schätzen Schweizer Unternehmen die Bedrohungslage durch Cyberangriffe ein?
Damit verzeichnet die Schweiz in der gesamten DACH Region den höchsten Zuwachs an Cyberangriffen.



Gemäss einer Studien stufen Dreiviertel (74 Prozent) der befragten Teilnehmer von Schweizer Unternehmen die aktuelle Bedrohungslage für die Cybersicherheit innerhalb ihrer Organisation als „hoch“ ein.



Mehr als die Hälfte (60 Prozent) glauben nicht daran, dass die interne Expertise zum IT-Sicherheitsfachwissen ausreiche, um das eigene Unternehmen vollumfänglich vor Cyberrisiken zu schützen.



78 Prozent der Schweizer Unternehmen erlebten mindestens einen Cyberangriff auf ihre IT-Infrastruktur während der Covid-19 Pandemie.

Kapersky-Umfrage unter Entscheidungsträgern in der Gesundheitsbranche, Mai 2021

Die sehr vulnerablen Systeme im Gesundheitswesen müssen präventiv vor Schadprogrammen und Cyberattacken geschützt werden, denn Datendiebstahl oder ein Ransomware-Angriff können das Vertrauen der Patienten in das Spital schmälern oder langfristig schädigen.

Ein Bug Bounty Programm ist für einen leistungsstarken Cyberschutz für vulnerable Systeme im Healthcare-Bereich entscheidend

Es braucht angepasste Schutzmassnahmen für die Gewährleistung der Sicherheit von Spitälern und anderen Pflegeeinrichtungen, denn Störungen, Ausfälle oder Sabotage des IT-Systems gefährden hier direkt die Gesundheit des Einzelnen. Das Universitätsspital Zürich setzt deshalb als eines der ersten Spitäler auf eine neue Testmethode. **Mit Hilfe von ethischen Hackern werden die IT-Systeme auf mögliche Sicherheitslücken geprüft.** Das Universitätsspital investiert sehr viel in den Bereich Sicherheit. Es geht darum proaktiv die Resilienz des Unternehmens zu erhöhen und nicht nur mit einer passiven Abwehrhaltung.

Im Universitätsspital wurde deshalb ein erster Reality Check beim Roll-out der neuen Webpage durchgeführt. „Der «Pilot-Testlauf war sehr erfolgreich. **Die ethischen Hacker haben Lücken gefunden, die sonst niemand vorher, auch nicht während den Pentests, entdeckt wurden.** Dabei haben wir festgestellt, dass die neuen Systeme den Tests standhalten, die älteren Systeme jedoch anfälliger sind. Bei den alten Systemen waren Lücken vorhanden, die wir schliessen mussten. Es ist immer besser mit «Good Guys» die Lücken zu finden und zu schliessen, als wenn dann «Bad Guys» die Schwachstellen entdecken.» fasst Erik Dinkel vom Universitätsspital zusammen.

«Ich finde Bug Bounty ist eine der effizientesten Arten, um sich vor Cyberattacken zu schützen, denn es ist echt. Es sind echte Menschen bzw. ethische Hacker dahinter, die das System in der Realität testen, dies generiert echte Findings und Resulate. Bug Bounty ist somit die beste Methode für einen Stresstest unter realen Bedingungen. Zudem ist es kosteneffizient, da erst gezahlt wird, wenn man etwas findet, im Vergleich zu Penetrationstests.»

Erik Dinkel *M.A. Chief Information Security Officer (CISO) des Universitätsspitals Zürich*

Dank der Arbeit der ethischen Hacker und den zur Verfügung gestellten **Reproduktionsanleitungen** konnten die gefundenen Sicherheitslücken entsprechend bearbeitet und geschlossen werden.

Aufgrund der Erfahrungen aus dem Pilotprojekt wurde ein längerer Proof of Concept gemacht. Ein kontinuierliches Bug Bounty Programm soll nun zu einem fixen Bestandteil der langfristigen Cyberschutz-Strategie des Spitals werden. Erik Dinkel fasst zusammen: «Bug Bounty ist nicht ein One-off, sondern muss etwas Kontinuierliches sein. Testing und Retesting müssen kontinuierlich sein. Wenn wir eine Lücke haben, möchten wir diese Lücke natürlich sofort schliessen. Ich sehe die kontinuierliche Überprüfung des Dispositivs als langfristige Massnahme. Auch wenn ich neue Entwicklungen habe, möchte ich diese gleich dem realen Stresstest unterziehen.» Beim Universitätsspital werden nun deshalb entsprechende interne Prozesse aufgesetzt und aufgebaut. Es wird mit einer Bug Bounty Plattform gearbeitet, welche in das Security Operating Center integriert wird.

Bug Bounty eignet sich für besonders exponierte Unternehmen, welche zur kritischen Infrastruktur gehören

«Im Grundprinzip geht es um «Schützen und Erkennen» und um richtig zu schützen, wird Erkennen in der Zukunft immer wichtiger werden. Die Frage ist nicht, ob du angegriffen wirst, sondern wann. Hier gilt es sofort zu reagieren, bevor Schaden entsteht.»

Erik Dinkel *M.A. Chief Information Security Officer (CISO) des Universitätsspitals Zürich*

Je mehr ein Unternehmen exponiert ist und zur kritischen Infrastruktur gehört, je mehr die eigenen Systeme mit dem Internet verbunden sind, umso höher ist das Risiko angegriffen zu werden. Deshalb ist ein Bug Bounty Programm insbesondere für die Gesundheitsbranche empfehlenswert. Erik Dinkel empfiehlt: «Ich würde jedem sicher einen ersten Test empfehlen, um sich einen Überblick zu verschaffen.

Nur höchste Sicherheitsanforderungen gewährleisten schlussendlich den Patienten- und Datenschutz. Deshalb bereitet sich das Universitätsspital mit einer Eventualplanung auf den Ernstfall vor. Hier gehört eben auch ein Stresstest mit ethischen Hackern unter möglichst realen Bedingungen dazu, um entsprechend schnell reagieren zu können und genau an diesem Punkt setzt das Bug Bounty Programm an.

«Schützen allein reicht nicht. Man sollte den Angreifern einen Schritt voraus sein und sich mit Hilfe der «Good Guys» proaktiv vorbereiten. Eine erfolgreiche Abwehr eines Angriffs muss vorbereitet werden.»

Fabian Kälin *Analyst Security Operating Center des Universitätsspitals Zürich*