Red Teaming: Cyber Resilience, War Gaming und Krisenmanagement

Abwehrkräfte stärken

Sascha Herzog, Michael Bartsch

Red Team Exercises sind ein wichtiger Baustein zur Beurteilung der eigenen Widerstandsfähigkeit gegenüber Cyberangriffen (Cyber Resilience). Aber was tun, wenn es trotzdem passiert und man von einem Angriff überrascht wird? Um das zu beantworten, gibt es diesmal Unterstützung von einem erfahrenen Krisenmanager als Co-Autor.

Ein Krisenmanager unterstützt die Opfer in der heißen Phase eines Cyberangriffs. Insbesondere für Unternehmen ohne größere, kompetente IT-Abteilung ist ein externer Krisenmanager häufig die einzige Möglichkeit, den Vorfall professionell zu handhaben und die Schäden und Auswirkungen zu begrenzen. Seine Aufgaben sind vielfältig und reichen von der Forensik, dem eigentlichen Incident Handling, Koordinieren von Hardware-, Software- und Servicepartnern, Datenschutz, Strafverfolgung und Wiederherstellungsplanung bis zur Mitarbeiter- und Kundenkommunikation. Gerade für kleine und mittlere Unternehmen kann ein professioneller Cyberangriff nervenaufreibend sein, da sie oft nicht wissen, an wen sie sich auf der Suche nach Unterstützung wenden können. Es mangelt hier nicht nur an gut ausgebildeten Mitarbeitern, sondern meistens auch an einem rechtzeitig aufgebauten Netzwerk an IT- und Security-Experten mit entsprechenden Verträgen, die dann schnell helfen können.

Aber auch Staaten, Behörden und große Firmen bis hin zu globalen Konzernen stehen bisweilen mit falschen Vorstellungen vor einem Angriff und wissen häufig auch nicht, was zu tun ist. Viele versuchen, den Angriffen mit Masse zu begegnen, und binden jeden Security-Experten ein, den sie finden können. Wenn dann herauskommt, wie teuer der Angriff war, wer alles an der großartigen Arbeit beteiligt war und dass sogar das Bundesamt für Sicherheit in der Informationstechnik (BSI) geholfen hat, mündet die Krise für alle Beteiligten in einen tollen Erfolg – besonders für den Angreifer. Und der hatte es vielleicht nicht einmal auf eine bestimmte Organisation abgesehen, sondern willkürlich einen Verschlüsselungstrojaner oder eine Ransomware in Umlauf gebracht.

Offizielle Ermittlungen sind selten

Ob sorgfältig ausgewählt oder zufällig betroffen: Anzeige erstatten die wenigsten Opfer. Meistens wissen sie gar nicht, dass jedes Bundesland in den Landeskriminalämtern sowie das Bundeskriminalamt eine Zentrale Ansprechstelle Cybercrime (ZAC) unterhält, die rund um die Uhr erreichbar ist. Dabei hat die Polizei Fähigkeiten und darf Maßnahmen ergreifen, die sonst niemandem zur Verfügung stehen. Das Ziel sollte ja sein, die Täter zu stellen und nicht nur die technischen Auswirkungen zu beseitigen.

Ein Krisenmanager unterstützt betroffene Unternehmen beim aufwendigen Zusammenspiel mit den Strafverfolgern. Er fungiert als Schnittstelle zwischen allen Beteiligten von den internen und externen Experten im Unternehmen, der Strafverfolgung bis hin zur Zusammenarbeit mit den Nachrichtendiensten. Der Angreifer ist ja nicht immer ein finanziell motivierter Cyberkrimineller, sondern er kann auch ein staatlicher Akteur oder ein rachsüchtiger Mitarbeiter sein. Daher ist es umso wichtiger, die Motive der Täter herauszufinden. Dazu erstellen die Beteiligten eine an Cyberstraftaten angepasste Verbrechenskartierung (Crime Map), die alle Aspekte des Angriffs erfasst und über ein Ausschlussverfahren das Tatmotiv ermittelt. Neben Details über technische Schutzvorkehrungen fließen Fakten über das Unternehmen wie Finanzdaten, Kunden- und Konkurrenzsituation, die Lieferketten der Produkte und Services, die Mitarbeitersituationen und Partner- und Lieferantenverbindungen in die Analyse ein. Dieses Vorgehen führt meist schneller zu einer Feststellung des Täters als die reine technische Analyse des Vorfalls.

Wenn es keinen Kontakt zum Täter gibt, hilft zumindest die Crime Map, den Angriff zu analysieren. Erst wenn eine Ursache feststeht, kann man die richtigen technischen und organisatorischen Entscheidungen treffen, die den Angriff möglichst vereiteln.

Übung und Simulation

Red Team Exercises helfen einem Unternehmen, Schwachstellen in der Abwehrfähigkeit in den Bereichen Mensch, Prozesse und Technik aufzudecken und zu zeigen, wie sich diese ausnutzen lassen, um kritische Geschäftsfunktionen (Critical Functions) zu kompromittieren. Diese Vorgehensweise kann die Abwehrbereitschaft steigern. Eine strategische Simulation als „Cyber Security War Game" wiederum ist eine Art Penetrationstest der rein organisatorischen Fähigkeiten einer Firma, die dabei die Führungsfähigkeit der handelnden Personen auf eine harte Probe stellt.

Cyber War Games werden zurzeit von vielen angeblichen Experten angeboten, jedoch steckt der Teufel hier im Detail. Erfahrungen aus dem Umgang mit tatsächlichen Krisen helfen bei der Entwicklung solcher Szenarien, da echte Vorfälle in die Szenarioentwicklung einfließen und somit ein praxisnaher und nicht theoretischer Ansatz des War Game zugrunde liegt. In den meisten Fällen sind die Unternehmen von den Szenarien überrascht und überfordert zugleich.

Als realistisches Test- und Übungsszenario dient im Folgenden dieser gezielte Angriff auf die Produktentwicklung eines Maschinenbauunternehmens: Unbekannten Tätern ist es gelungen, den Firmware-Quellcode der im wichtigsten Produkt eingesetzten Prozessoren zu manipulieren. Beim nächsten Update wäre eine Fehlfunktion die Folge und weitere Updates würden blockiert, was Rückrufaktionen und erhebliche Kosten nach sich zöge.

Dieses Fehlverhalten wollen die Täter kurz vor entscheidenden Vertragsverhandlungen mit einem wichtigen Kunden provozieren und öffentlich machen. Anhand einer Crime Map können die Ermittler analysieren, wie die Angreifer bisher vorgingen und worin ihr Ziel besteht: eine Verschiebung der Wettbewerbsposition.

Das auf tatsächlichen Geschehnissen basierende Szenario dient als Grundlage für eine kombinierte Übung. Sie könnte ungefähr wie folgt ablaufen und würde mit einer War-Game-Phase beginnen, nämlich einer Analyse der Marktposition und der Verträge mit Kunden und Lieferanten, der Patente, Produkteigenschaften und Verflechtungen der Firmenstrukturen und deren Eigentümer (Open Source and Financial Intelligence). Mehr ins Detail geht das Herausfinden branchenspezifischer Kommunikationsmedien und -kanäle, eine Umfeldanalyse der gesamten Supply Chain der jeweiligen Produkte. Hier kristallisiert sich bereits der bestmögliche Zeitpunkt eines Angriffs heraus.

Praxisbeispiel: Manipulation von Firmware

Nun beginnt das Red Team den simulierten Angriff mit einer taktischen Informationsbeschaffung [1] zu den Personengruppen und Dienstleistern, die mit der Software- und Firmware-Entwicklung zu tun haben, sowie zu Zulieferern und weiteren „Trusted Parties" in diesem Bereich.

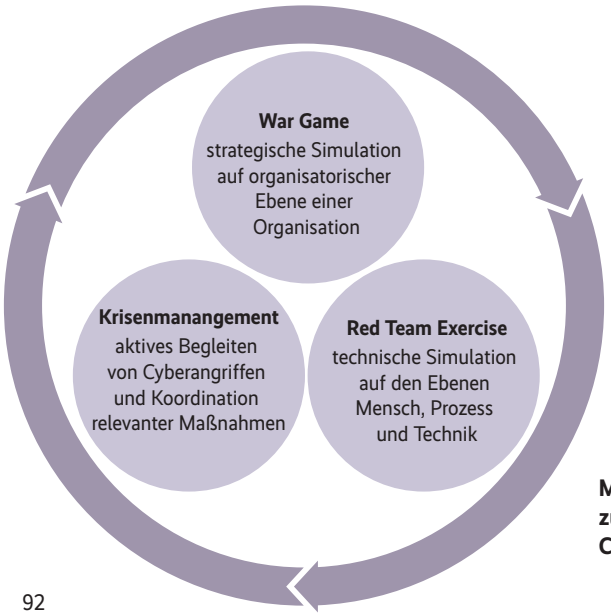
Der nächste Schritt besteht in der Inventarisierung relevanter externer Systeme, ebenfalls mit einem Fokus auf den Bereich Software-/Firmware-Entwicklung, gegebenenfalls mit gezielten Exploit-Versuchen und weiteren direkten Angriffen auf vielversprechend erscheinende Ziele.

Spear Phishing ergänzt physische Einbruchsversuche

Es folgen Versuche, nicht technische Mitarbeiter in einem Bereich wie Buchhaltung, Einkauf, Marketing oder Personalverwaltung mittels Phishing anzugreifen, um bei einem Fehlschlag davon abzulenken, dass die Entwicklungsabteilung das eigentliche Ziel ist. Zusätzlich (oder alternativ) zum „Spear Phishing" [1] könnte man versuchen, schlecht gesicherte Gebäude zu betreten, die möglichst ans Intranet und Active Directory angeschlossen sein sollten, um hier über eine unscheinbare Hardware mit einer integrierten SIM-Karte einen dauerhaften, schwer zu lokalisierenden Zugang zu etablieren. Sollten beide Einbruchsversuche scheitern, bleibt die Möglichkeit, die zuvor ausfindig gemachten Entwickler respektive deren Rechner direkt über Phishingangriffe zu kompromittieren.

Sobald der Zugang ins interne Netz steht, installiert das Red Team einen gesicherten, persistenten C2-Kanal (C&C, Command and Control, [1]) und versucht erst einmal nur, unbemerkt zu bleiben. Mit den ebenfalls bereits in einem früheren Artikel beschriebenen Methoden der „Post Exploitation" und des „Lateral Movement" [1] würde es die Entwicklungssysteme und gegebenenfalls die Entwickler bei der täglichen Arbeit beobachten, um die Prozesse des Software-Deployments und Abläufe aufzudecken, die sich für eine Manipulation eignen. (Achtung: Dies ist innerhalb der EU aus Gründen des Datenschutzes heikel, was tatsächliche Angreifer jedoch nicht stört.) Ist eine solche Möglichkeit gefunden, beweisen wir in enger Koordination mit dem Kunden, dass tatsächlich eine Manipulationsmöglichkeit der Firmware existierte (Proof of Concept, etwa mittels Manipulationen der Versionsverwaltungssysteme).

Nach Auslieferung des Berichts und einem Abschluss-Workshop mit Managern, Technikern und Projektleitern auf Kundenseite steht ein sogenanntes „Replay" an, eine Wiederholung der einzelnen Angriffsphasen, um zu testen, ob das „Blue Team" des Kunden anhand unserer Maßnahmen seine Widerstandsfähigkeit gegenüber solchen Angriffen so weit verbessern konnte, dass wir mit ähnlichen



Maßnahmen zur Vorbeugung von Cyberangriffen

Angriffen nicht erneut und vor allem nicht unerkannt durchkommen.

Auf Basis der bisher gewonnenen technischen Erkenntnisse können als Training und Vertiefung weitere strategische Simulationen etwa in Form eines „Cyber Security War Game“ folgen – zum Aufdecken der organisatorischen Schwachstellen in den Bereichen Prävention, Reaktion, Wiederherstellung. Zusätzliche simulierte, aber gezielte technische Angriffe auf kritische Geschäftsprozesse (Critical Functions) in Form von „Red Team Assessments“ sind ebenfalls sinnvoll.

Aufgrund des koordinierten Incident Handling im realen Beispielszenario ließen sich im Zusammenspiel aller Beteiligten größere Schäden und das Ausführen der Schadroutinen verhindern. Das realistische, aber stark vereinfachte Szenario verdeutlicht, wie wichtig es ist, auf solche Fälle vorbereitet zu sein und die geeignete Unterstützung für den gesamten Angriffszyklus im Voraus zu planen. Nach dieser Übung konnte das betroffene Unternehmen auch gleich die Qualitätsverbesserung in den Entwicklungsprozessen von Soft- und Hardwareprodukten umsetzen, um ähnliche, echte Angriffe zukünftig abzuwehren.

Simulierter Angriff erfolgreich abgewehrt

Da der Kunde des „War Game“ ein solches Szenario zuvor nicht berücksichtigt hatte, waren auch die Verträge mit externen Partnern, Lieferanten und Kunden daran anzupassen und ein gemeinsames Risikomodell für die gesamte Supply Chain zu entwickeln. Die Governance für Cybersecurity erfuhr ebenfalls Änderungen und die Beteiligten erstellten ein Krisenhandbuch.

Momentan plant das Unternehmen weitere War Games und Red Team Assessments, um auf den nächsten Ernstfall besser vorbereitet zu sein. Je nach den Fähigkeiten der Angreifer lassen sich Vorfälle ab einem gewissen Niveau natürlich nicht immer vollständig abwehren. Sie sollten allerdings anhand der vorbereiteten Szenarien und umgesetzten Maßnahmen (Technik, Prozesse, Awareness) zumindest detektierbar und schnell einzudämmen sein. Durch die Kombination aus War Game, Red Team Exercise und einem professionellen Krisenmanagement kann man sich optimal auf solche Angriffe vorbereiten, um das Schlimmste zu verhindern und als Unternehmen nur eine geringe Angriffsfläche für Cyberangriffe zu bieten. (un@ix.de)

Sascha Herzog

ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.

Michael Bartsch

ist Geschäftsführer der Deutor Cyber Security Solutions. Er berät Staaten und Unternehmen bei der Risikovorsorge sowie technischen und organisatorischen Sicherheitsmaßnahmen.

Quellen

[1] Die vorangegangenen Artikel von Sascha Herzog zu Themen wie Lateral Movement, Command and Control oder Spear Phishing finden sich unter ix.de/ix1904091.