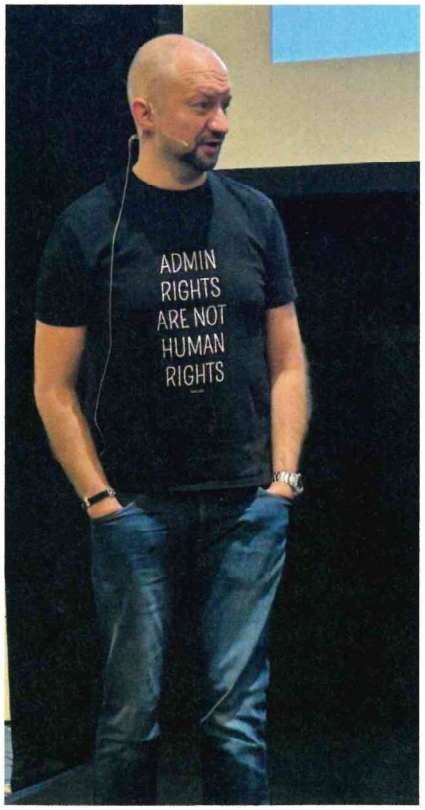
Kontraproduktiv: Viele Opfer von Cybercrime halten sich bedeckt

Bei der diesjährigen IT-Defense fiel die Bestandsaufnahme der Securityexperten in Sachen Cybercrime alles andere als ermutigend aus. Hoffnung machen allerdings Erfolgsgeschichten wie die Zerschlagung des Erpressernetzwerks Hive durch deutsche und internationale Fahnder.

Von Jörg Riether

Vom 31. Januar bis 2. Februar 2024 fand in Stuttgart die IT-Sicherheitskonferenz IT-Defense des Heilbronner Unternehmens Cirosec statt. IT-Sicherheits-Urgestein Sami Laiho fasste in seiner Keynote „Forward to the Past and Back to the Future – Cybercrime in 2024 and Beyond" die weltweite Situation im Bereich Cybercrime zusammen.

Für das Jahr 2023 warf er provokativ drei Zahlen an die Wand: 2, 180 und 2. Jede dieser Zahlen sei erschreckend und insbesondere die letzte außerordentlich traurig. Im Detail steht die erste Zahl für zwei Stunden, die durchschnittliche Zeitspanne, die ein Angreifer benötigt, um ab seinem Eindringen ins Unternehmensnetz Domänenadminrechte zu erlangen. Die zweite Zahl steht für 180 Tage. Das ist die durchschnittliche Zeit, die Angreifer sich leise im Netz verhalten, bevor sie final zuschlagen. Gerade angesichts der Standardeinstellung vieler Detektionsprodukte, die mit Log-Aufbewahrungszeiten von nur 30 Tagen arbeiten, sollte man dies unbedingt im Hinterkopf behalten, so Laiho.



Die Cybercrime-Bestandsaufnahme des Securityexperten Sami Laiho fiel wenig optimistisch aus (Abb. 1).

Die letzte Zahl steht für 2 Prozent, und zwar für 2 Prozent aller erfolgreich angegriffenen Opfer. Nur so wenige würden an die Öffentlichkeit gehen und darüber sprechen, alle anderen halten es geheim. Insofern ist dies auch gleichzeitig die traurigste Zahl, denn es macht die Gesamtsituation extrem schwierig für IT-Sicherheitspersonal. Durch diese absurd niedrige Zahl könnte bei vielen Vorständen die Illusion entstehen, dass es gar kein so großes Problem gibt, weil man kaum etwas liest und hört.

Mikko spricht jetzt türkisch

Zu neuen Manipulationstechniken zeigte Laiho ein Deepfake-Video, für das eine relativ einfache Nvidia-Home-Konfiguration benutzt wurde, um optisch perfekt und nicht als Fälschung erkennbar dem bekannten finnischen Sicherheitsexperten Mikko Hypponen einen türkischen Text passend zu seinen Gesichtsbewegungen unterzuschieben (siehe ix.de/zrda).

Laiho zeigte außerdem eine Version von sich selbst, die mit einer SaaS-Software und einer einfachen Webcam erzeugt wurde und in der er aus Sicherheitssicht haarsträubende Dinge erzählte – allerdings in perfektem Englisch und danach in perfektem und akzentfreiem Deutsch. Es ist erschreckend, wie absurd einfach es heutzutage ist, solche Deepfakes zu erzeugen. Für sein eigenes Beispiel hatte Laiho das System von HeyGen benutzt (siehe ix.de/zrda).

Laiho gab aus seiner Sicht wesentliche Empfehlungen zur Verbesserung der Sicherheit, Stand 2024. Ganz oben auf seiner Liste steht eine strukturierte Tiering-Systematik, die man etablieren und einhalten soll, etwa die strikte VLAN-Zuweisung zwischen fachlichen Admins X und beabsichtigten Fachsystemen Y (siehe Abbildung 2). So sollen beispielsweise Backup-Admins ausschließlich auf Backup-Systeme zugreifen dürfen und auf nichts anderes, sie sollen nicht einmal aus dem dedizierten Backup-VLAN ausbrechen dürfen. Das bedeutet auch, dass etwa ein Domänenadminkonto auf Tier 0 nur auf Domänencontroller, PKI und PIM-Systeme zugreifen, sich aber niemals auf nachgelagerten Tier-1- und -2-Systemen wie normalen Servern oder gar Workstations anmelden kann.

Laiho wies in diesem Zusammenhang mit Nachdruck darauf hin, unbedingt Backups mit Immutable-Technik (künstliche Unlöschbarkeit) zu benutzen. Ich würde hier sogar noch einen Schritt weiter gehen und empfehlen, sofern es Anforderungen und Ressourcen erlauben, zusätzlich zu Online-Immutable-Systemen mit echten Air Gaps (also isolierten Backups) zu arbeiten.

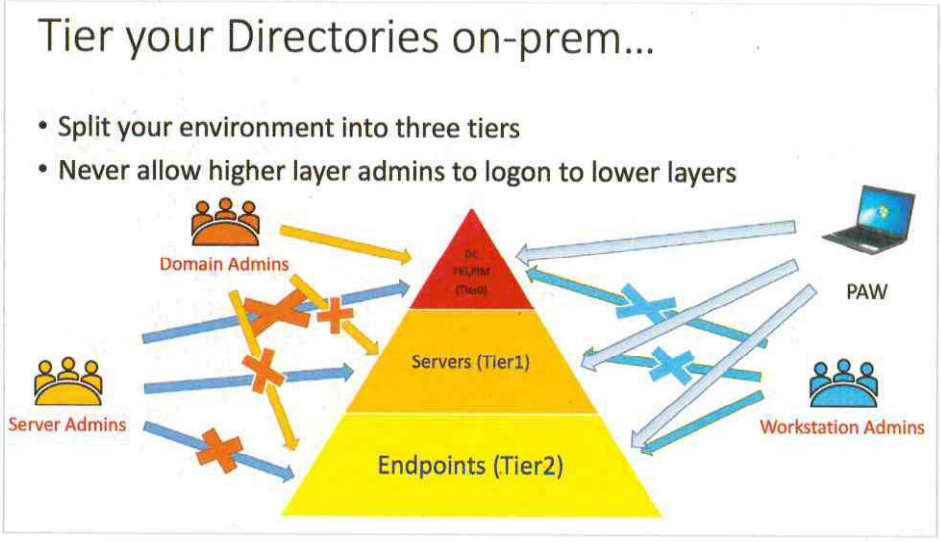
RDP = Ransomware Deployment Protocol

Extern angreifbare Systeme standen ebenfalls ganz oben auf Laihos Gefahrenliste. Die Suchmaschine Shodan ist inzwischen derart schnell und verteilt, dass sie alle vier Minuten das gesamte IPv4-Internet durchsuchen kann. Veröffentlicht man also heute eine neue extern erreichbare Instanz, würde es lediglich vier Minuten dauern, bevor diese von Shodan geprüft wird.

Der Klassiker sind hier von außen erreichbare RDP-Zugänge, so Laiho. Er bezeichnete RDP scherzhaft als Ransomware Deployment Protocol. 80 Prozent der direkten Ransomware-Attacken auf externe Systeme würden auf RDP zielen.

Damit dürfte er nicht ganz falsch liegen. Man muss sich in der Tat nur einmal auf Shodan öffentlich auf Port 3389 erreichbare Systeme in Deutschland anschauen.

Als weitere wichtige Maßnahme für 2024 empfahl Laiho wörtlich: „Patch More, Test Less!" So schlimm sich dies auch anhöre, die Situation sei inzwischen so, dass man sich den Luxus von guten Tests nicht mehr leisten könne – extrem schnelles Patchen sei mit Abstand das geringere Risiko. Man hat hier nur exakt zwei Optionen: nämlich entweder zwei Stunden Downtime, um ein Update zu installieren oder schlimmstenfalls ein fehlerhaftes Update zu reparieren, oder mindestens drei Monate Downtime durch einen schnellen Angriff, weil man nicht sofort nach einem Update-Release reagiert hat.



Im Kern eines guten Sicherheitskonzepts steht ein restriktives Tiering-Modell, das gerade Admins keinen Zugriff auf andere Fachsysteme erlaubt, auch nicht auf hierarchisch weiter unten befindliche (Abb. 2).

Was ist TOCTOU?

Ein echtes Techie-Highlight war der Vortrag „Uninstalling Security: Local Privilege Escalation durch Symbolic Links" von Frederik Reiter und Jan-Luca Gruber. Lokale Rechteausweitungen (Local Privilege Escalation, LPE) sind bekanntlich ein wesentliches Element bei Angriffen auf IT-Strukturen. Reiter und Gruber beschäftigten sich mit sogenannten Time-of-Check-/Time-of-Use-Schwachstellen, in der Community gerne als TOCTOU bezeichnet. Solche Schwachstellentypen sind zwar nicht neu, aber relativ wenig öffentlich beachtet.

Ein sehr vereinfachtes Beispiel würde so aussehen, dass man etwa eine Laufzeitbibliothek eines hochprivilegierten Prozesses zur Laufzeit mal eben gegen

eigenen beliebigen Code austauscht, wohl wissend, dass dieser in der Regel auch auf gültige Signaturen hin geprüft wird, man also vermeintlich in einer Sackgasse landet. Was wäre aber nun, wenn man die DLL trotzdem austauschen könnte, aber erst nach der Signaturprüfung, damit die Prüfung nicht fehlschlägt?

Jedoch hätte man dafür allenfalls Mikrosekunden Zeit, also wieder ein wenig praktikables bis unmögliches Unterfangen. Also eine weitere Sackgasse? Nein, denn der Trick geht ganz vereinfacht gesagt so, dass man auf Windows-Systemen via Opportunistic Locks die DLL festhält. Davon hat man sie aber noch lange nicht ausgetauscht, dies trickst und löst man durch geschicktes Ausnutzen von NTFS-Junctions und Symbolic Links.

Die kompletten weiteren Details dieser und eng verwandter Techniken würden den Artikel sprengen; gleichwohl muss erwähnt werden, dass in diesem Zusammenhang durch die Forschung der beiden Vortragenden auch CVE 2023-38041 das Licht der Welt erblickte. Es stellt sich zum Erstaunen der Zuhörer heraus, dass dies eine der im Netz prominent aufgegriffenen Ivanti-Schwachstellen betrifft, um genau zu sein die Ivanti Secure Access Client LPE (siehe ix.de/zrda).

Polizei am Puls der Zeit

Daniel Lorch, Ermittlungsleiter der Cybercrime im Polizeipräsidium Reutlingen, Baden-Württemberg, sprach offen und sympathisch-entwaffnend über seine Arbeit. Er verwies zunächst auf die Schadensbilanz 2022 in Deutschland, der zufolge der deutschen Wirtschaft durch Angriffe auf Unternehmen ein Schaden von 203 Milliarden Euro entstanden war – also fast der halbe Bundeshaushalt. Die Zahlen stammen aus einer Studie des Bitkom (siehe ix.de/zrda).

Wenn man eine Cyberattacke als betroffene Person nicht schon einmal selbst erlebt hat, kann man sich die unmittelbaren und folgenden Auswirkungen kaum vorstellen, sagte Lorch. Man sollte sich dringend mit anderen Unternehmen vertraulich vernetzen und wenn möglich auch mit ehemals Betroffenen sprechen. Er berichtete von einem Unternehmen, das am Freitagabend noch existierte, am Montagmorgen aufgrund einer Cyberattacke aber nicht mehr. Was eine solche traumatische Erfahrung mit den Menschen macht, könne man sich aus der Entfernung nicht einmal ansatzweise vorstellen.

Lorch sagte, dass als Gegenmaßnahme für Ransomware-Angriffe ein einfaches Application Whitelisting wie AppLocker schon eine große Hilfe sei. Es gab tatsächlich einen konkreten Fall, an den er sich erinnerte, bei dem diese Mitigation letztlich wirksam war und Schlimmeres verhindert hatte. Sogenannte Ransomware-sichere Online-Backups, die dieser Tage häufig beworben werden, bezeichnete er als Paradoxon und traf damit einen Nerv der zuhörenden Community.

Er empfahl zudem dringend, interne Geschäftsdaten abzusichern. Wenn etwa eine Hotelkette gehackt wird und es stellt sich dann heraus, dass Kreditkartendaten von Kunden völlig unverschlüsselt dort gespeichert waren und nun im Darknet veröffentlicht sind, kann einem schon angst und bange werden. Lorch rät dazu, im Fall eines erfolgreichen Angriffs sofort die Kriminalpolizei einzuschalten. Diese habe heute echte technische Möglichkeiten, das Ziel des Datenabflusses zu detektieren und zuweilen sogar etwaiges Datenhosting der Kriminellen einzufrieren.

Hive: Die Kriminellen gewinnen nicht immer

Lorch war maßgeblich an einer weltweit koordinierten Operation zur Enttarnung und Zerschlagung der seit Juni 2021 in Erscheinung getretenen Ransomware-as-a-Service-Gruppe Hive beteiligt. Diese skrupellosen kriminellen Akteure, die schwerpunktmäßig Schulen, Universitäten, Rechtsanwälte, Behörden und Krankenhäuser nahezu weltweit attackierten, waren für über 1500 Angriffe in 88 Ländern verantwortlich. Schrecklich zu erfahren war, dass bestätigt mindestens drei Personen aufgrund der Krankenhausangriffe verstarben.

Die Geschichte zur Zerschlagung der Gruppe ist indes bemerkenswert. Man habe mit deutschen gültigen Beschlüssen die Gruppe beobachtet, es sei ausdrücklich kein Hackback gewesen. Im Rahmen der Ermittlungen ist man dann auf Schlüssel gestoßen, mit denen man Daten bei Opfern entschlüsseln konnte. Lorch und die beteiligten internationalen Teams sind sodann auf die Opfer zugegangen und haben ihnen geholfen – immer alles bei gleichzeitiger Wahrung der höchsten Vertraulichkeit, damit man heimlich die Gruppe weiterverfolgen und sie im Glauben lassen konnte, dass niemand hinter ihnen her war.

Die Polizeiarbeit war schließlich erfolgreich und Lorch berichtete, dass die Infrastruktur von Hive mindestens beachtlich war. Sogar das Justizministerium der Vereinigten Staaten gab dazu ein offizielles Statement ab und bedankte sich gemeinsam mit der FBI-Direktion vor laufender Kamera für die international koordinierte Polizeiarbeit. FBI-Direktor Christopher Wray höchstpersönlich lobte in seinem Statement die gute Arbeit der Polizei Reutlingen (Videoaufzeichnung siehe ix.de/zrda).

Die kommende IT-Defense wird vom 12. bis 14. Februar 2025 in Leipzig stattfinden. (ur@ix.de)

Die „Homepage" nach dem Ermittlungserfolg (Abb. 3).