IT-Revision

Christian Schülke

Security Information and Event Management

Einleitung

Wie schön wäre es, wenn wir ein vollständiges Lagebild unserer IT-Systeme haben könnten? Sämtliche Systemzustände, aktuelle und historische Auslastung sowie selbstverständlich die aktuell laufenden Angriffe samt ihrer hoffentlich erfolgreichen Abwehrmaßnahmen.

Die Echtzeitanalyse und übergreifende Korrelation liefert für Incident Response Fälle eine Bewertung sowie die zugrundeliegenden Daten. Durch Langzeitarchivierung aller Events lassen sich historische Auswertungen erstellen und Trends ermitteln, die fundierte Entscheidung ermöglichen, um für die Zukunft besser gewappnet zu sein.

Reports zur Erfüllung diverser Compliancevorgaben kann ein solches System ebenfalls liefern. Dieser Funktionsumfang ist sehr umfassend, wird aber von den relevanten Regelwerken mehr oder weniger direkt gefordert. Der IT-Grundschutz des BSI, die ISO 27000, PCI DSS etc. fordern eine Auswertung von Logdateien und Eventinformationen samt passender Bewertung und Bearbeitung.

Hinter dem Kürzel SIEM verbirgt sich ein komplexer Ansatz, um genau diese Ziele zu erreichen: Security Information and Event Management (SIEM) beschreitet diesen Weg, zu dem ich Ihnen nachfolgend wichtige Ideen und Ansätze vorstellen möchte.

Hintergrund und Voraussetzungen

Die Erkennung, ob ein System oder Dienst verfügbar ist, gestaltet sich sehr einfach. Performancewerte zu erfassen und zu bewerten ist ebenfalls nicht schwer. Aber wie sieht es aus, wenn bewertet werden soll, ob ein bestimmter Zugriff oder eine bestimmte Aktion gutartig oder böseartig ist?

Ein grundlegendes Element für solche Betrachtungen, auch über SIEM hinaus, ist das sogenannte Baselining und Profiling als Definition, wie die normale Nutzung aussieht. Unsere Schutzsysteme zielen in aller Regel darauf ab, uns un-

normale, auffällige und außergewöhnliche Situationen anzuzeigen. Wie aber kann ich eine solche Bewertung vornehmen, wenn der Normalzustand gar nicht ausreichend definiert ist?

Als Input hierfür dienen uns die vielen Sicherheitssysteme, die bereits im Netzwerk ihren Dienst verrichten: Firewalls und Antivirus, Intrusion-Detection-Systeme, Data-Leakage-Protection, Mobile-Device-Management u.a.m. Jeder Switch liefert wichtige Informationen, ob z.B. ein Kabel kurzzeitig ausgesteckt wurde, Router sehen jedes Datenpaket und Server führen Dateizugriffe oder Datenbanktransaktionen aus. Eine tiefergehende Betrachtung des Inhalts von Datenverbindungen oder des Verhaltens der Applikationen liefert zusätzliche Erkenntnisse. Alle diese Events sind wertvolle Informationen, die es gilt, als Gesamtbild zusammenzufassen und zu bewerten. (Abb. 1)

Ein praktisches Beispiel soll dies verdeutlichen:
Der Mitarbeiter erhält eine E-Mail mit einem PDF-Anhang, der eine neuartige Schadsoftware enthält.
Der Virenscanner verfügt noch nicht über das Wissen, diese zu erkennen.

Der Ablauf stellt sich im Detail wie folgt dar: (Abb. 2 auf S. 196)

- Die E-Mail kommt aus dem Internet am externen Gateway an und wird zum Empfangsmailserver durchgeleitet (der Emailempfang ist per Regel in der Firewall erlaubt, die FW kann diesen Verbindungsaufbau protokollieren)
- Der E-Mail-Server empfängt die Mail und kann Zeitpunkt und Dauer der Verbindung, Datenmenge, Absender und Empfänger sowie Art und Anzahl der Dateianhänge protokollieren. Der auf dem Server laufende Viren- und Malwarescanner erkennt keinen bösartigen Code in den Attachments
- Der Benutzer ruft die Mail mit seinem Client (PC oder Smartphone) ab, auch dieser Zugriff wird mit allen Details vom Server protokolliert
- Der Abruf des Clients kann auch vom Client selbst geloggt werden.
- Die Mail wird vom Benutzer gelesen und das Attachment geöffnet. Auch der lokale Virenscanner findet nichts Auffälliges und gibt die Datei frei, die daraufhin an den PDF-Viewer zur Anzeige übergeben wird. Dieser Vorgang lässt sich ebenfalls loggen.
- Die Schadsoftware kann eine Schwäche im Anzeigeprogramm (PDF Viewer) ausnutzen, worauf dieses nun z.B. mit einem Fehler abstürzt, der besagt, dass die Datei evtl. beschädigt ist. Auch das lässt sich protokollieren. Microsoft Office und andere Programme lassen ebenfalls eine solche Protokollierung zu.
- Im Hintergrund baut der jetzt aktiv gewordene Schadcode eine Verbindung zu einem System im Internet auf, mit dem höchstwahrscheinlich von diesem Client aus bislang noch keine Kommunikation geführt wurde. Dies würde die Firewall feststellen können, über den dieser Client ins Internet geht.

Die einzelnen Aktionen sind für sich genommen allesamt nicht kritisch. Der Mailempfang in seinen verschiedenen Stufen findet täglich unzählige Male statt.

Der Absturz des PDF-Viewers tritt zwar nicht sehr häufig auf, ist aber auch nicht ganz unbekannt. Es kommt in der Tat auch mal vor, dass eine Datei wirklich defekt ist. Der Aufbau von Verbindungen zu bislang unbekannten Systemen passiert bei jedem Aufruf einer Website, die vorher noch nie besucht wurde. Auch das ist für sich genommen nichts Ungewöhnliches.

Alles zusammen im zeitlichen Kontext betrachtet, ist allerdings als kritisch zu bewerten und zumindest zu

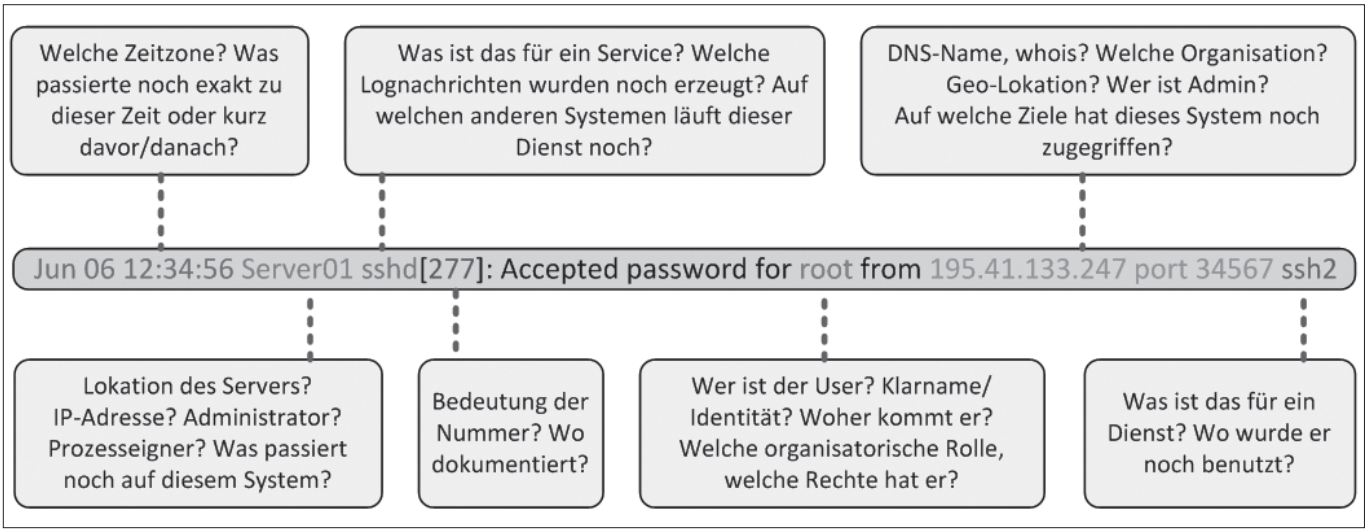

Abb. 1: Beispiel einer Logzeile mit Informationen und Fragen, die hierzu auftauchen könnten

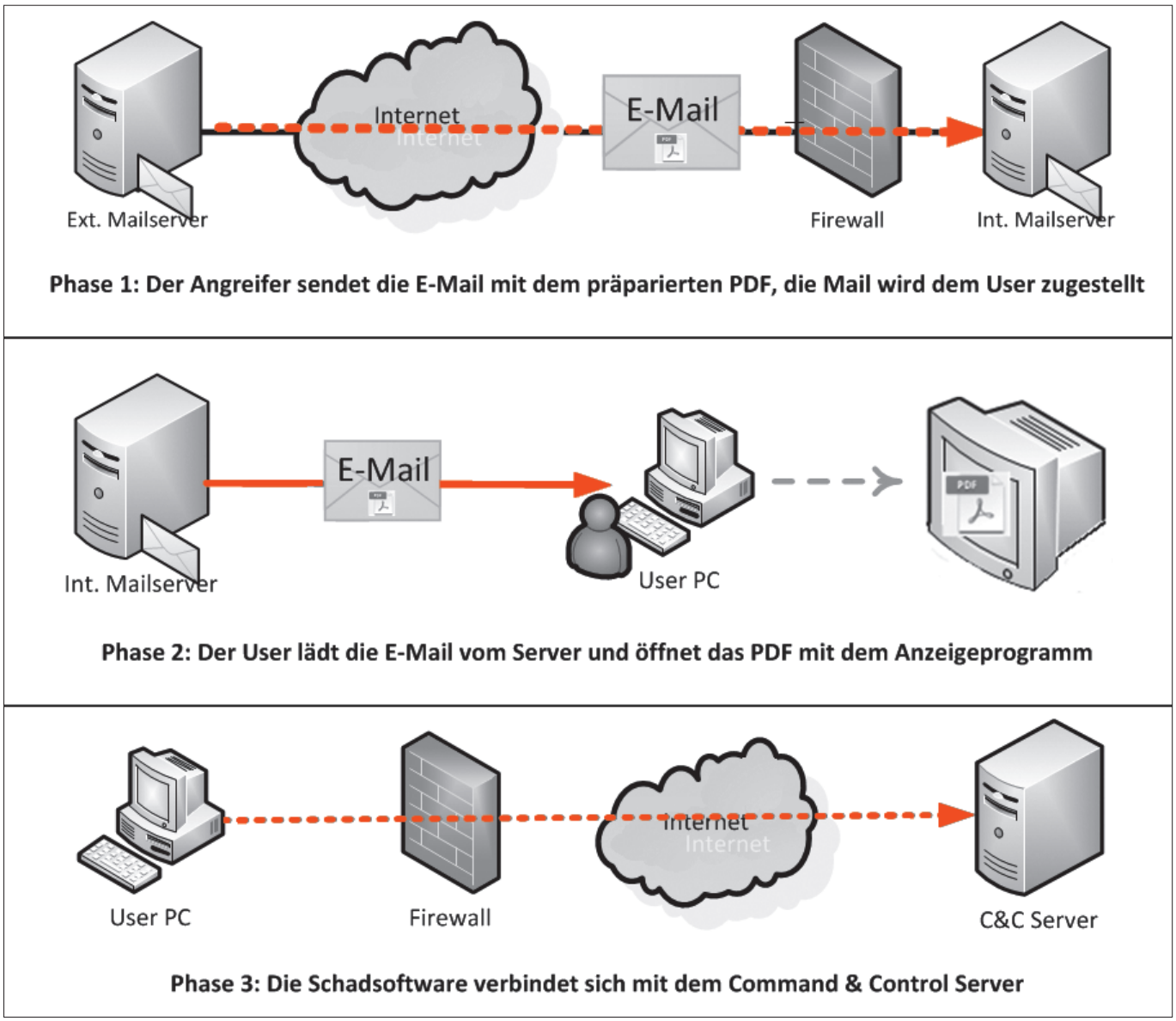

Abb. 2: Schaubild des Ablaufes

hinterfragen.

Es ist leicht erkennbar, dass viele dieser Informationsquellen schon in Unternehmen vorhanden sind. Die Vorteile eines SIEM liegen nun darin, die Informationen aus verschiedenen Quellen in eine zeitliche Reihenfolge zu bringen, Zusammenhänge darzustellen und auf Basis dieser und weiterer externer Informationen (z.B. IP-Liste bekannter Botnetz-Server) Handlungsempfehlungen zu geben. Je nach verwendeter Lösung wird auch direkt eine Filterung vorgenommen, die der IT-Abteilung hilft, den Blick auf das Wesentliche zu lenken.

Allerdings wird schon bei diesem Beispiel deutlich, dass die Implementierung einer solchen Lösung eine gewisse Zeit erfordert, da unternehmensspezifische Eigenheiten berücksichtigt werden müssen. Ferner erfordert der Betrieb eines solchen Systems eine regelmäßige Betreuung, da sich Angriffsszenarien sowie die interne IT-Landschaft permanent ändern.

Datenquellen

Das vorgestellte Beispiel zeigt lediglich einen kleinen Ausschnitt aus der Vielzahl der Bedrohungen. Die Frage ist, welche anderen Szenarien es noch gibt. Was muss wo und wie erkannt werden? Und wie sieht es mit der Dynamik aus, denn die Welt der Bedrohung ändert sich heutzutage leider sehr schnell. Angriffe können nicht nur von außen kommen, sondern häufig auch von innen. Oftmals sind diese aber gar nicht von dem jeweiligen Benutzer initiiert, sondern dessen Systemzugang wird missbraucht, weil es gelungen ist, im Vorfeld seine Anmeldedaten zu stehlen.

Lieferanten für wertvolle Informationen finden sich reichlich innerhalb der IT:

- Firewalls, sowohl netzwerk- als auch hostbasiert
- Intrusion Detection Systeme, ebenfalls netzwerk- und hostbasiert

- Flowdaten mit den Verbindungsdetails der einzelnen Netzwerkgeräte
- Logginginformationen von Servern und Datenbanken
- Systemlogs, z.B. Windows Eventlogs. Diese gibt es nicht nur auf Servern, sondern auch auf den Clientsystemen. Eine Sonderstellung stellen mobile Clients dar (Notebooks, Tablets und Smartphones), die besonders oft Ziel von Angriffen werden. Deren Logginginformationen können aber teilweise nur erheblich zeitversetzt erfasst werden, z.B. wenn der Benutzer mit seinem Gerät außerhalb des Unternehmensnetzwerks unterwegs ist
- Data Leakage Protection
- Mobile Device Management
- Systeme zur Überprüfung der Datei-Integrität

Als Einstieg sollen diese Quellen erst einmal genügen, eine Erweiterung um detailreichere Datenquellen ist im Betrieb jederzeit möglich und sinnvoll.

Für die Bewertungslogik all dieser zusammengeführten Einzelinformationen (Korrelation) gibt es verschiedene Quellen. Die Hersteller verteilen über Abonnements allgemeine Erkenntnisse, ähnlich den Signaturupdates bei Antivirensoftware. Aus den unternehmenseigenen Vorgaben und Vorkommnissen kommen individuelle Regeln hinzu. Zusätzlich sollten Informationen von Sicherheitsfirmen und Polizei-/Ermittlungsbehörden, sogenannte Indicators of Compromise (IoC), berücksichtigt werden. IoC können aus IP-Adressen, Zeichenfolgen, Hashwerten oder Programmcode bestehen. Dies sind harte Fakten, die an anderer Stelle ermittelt wurden und oft bei Vorfinden im eigenen IT-Verbund einen begründeten Verdacht für eine Infektion oder Kompromittierung nahelegen.

Betrieb

Wie bei jedem anderen automatischen, regelbasierten System kommt es auch bei einem SIEM zu Fehlalarmen (false positives). Gerade in der Einführungsphase muss das System noch an umgebungsspezifische Eigenheiten angepasst werden. Dieses ist eine nicht zu unterschätzende Aufgabe und der Zeitaufwand muss in der Implementierungsphase ausreichend berücksichtigt werden.

Bei der Auswahl eines geeigneten Produktes ist darauf zu achten, dass diese Feinjustierung nicht zu viel administrativen Aufwand erzeugt.

Im Falle eines Events kann das System automatisch alarmieren, sogar ein eigenständiges Eingreifen in Firewallregeln zur Unterbindung des verdächtigen Datenverkehrs wäre technisch möglich. Hierbei besteht jedoch die Gefahr, dass produktive Systeme durch eine vorschnelle oder falsche Bewertung vom Betrieb getrennt werden und dadurch Ausfallschäden entstehen. Welcher Schaden könnte entstehen, wenn z.B. das Shopsystem durch einen Fehler automatisch vom Internet getrennt würde und niemand mehr bestellen könnte?

Die Alarmierung im Fall eines schweren Regelverstoßes sollte dem Bearbeiter neben der übergeordneten Bewertung samt Begründung auch die zugrundeliegenden Daten liefern, sodass unmittelbar mit einer Analyse begonnen werden kann. Mit diesen Details können aus den historischen Daten auch andere betroffene Systeme herausgefiltert sowie Angriffswege und Ursprung von Infektionen ermittelt werden.

Es gibt noch weitere positive Ergebnisse, die der Einsatz einer solchen Lösung mit sich bringt.

Innerhalb des SIEM kann eine regelmäßige Inventarisierung aller an das Netzwerk angeschlossenen Systeme erfolgen. Wird im Netzwerk ein System erkannt, das nicht in der Inventarliste des SIEM vorhanden ist, kann dieses System bis zur Klärung in eine Quarantäne verschoben werden.

Aufgrund der im System vorliegenden Daten ist auch eine Echtzeiterkennung von Botnetz-Kommunikation sowie Verbindungen zu bösartigen Command&-Control-Servern möglich. Auch die Erkennung von ungewolltem Datenabfluss wäre darstellbar.

Wichtig für einen kontinuierlich erfolgreichen Betrieb ist ein sehr strikter Regelkreislauf. Dieser besteht ähnlich den bekannten PDCA-Zyklen aus Vorgabenerstellung, Einlernphase und Regelwerksanpassung, Erfolgskontrolle und Bewertung und dem Abgleich mit aktuellen Vorgaben.

Datenschutz

Der Datenschutz ist ein weiterer, sehr wichtiger Aspekt bei der Betrachtung einer solchen Lösung. Aufgrund der Vielzahl an detaillierten Daten wäre grundsätzlich eine fein granulierte Überwachung der Mitarbeiter möglich. Neben den technischen Möglichkeiten von Anonymisierung, Pseudonymisierung und 4- oder 6-Augen Prinzip bei Auswertung und Einsichtnahme (gemeinsam mit einem Datenschutzbeauftragten, Betriebsrat o.ä.) gilt es, bereits im Vorfeld den Einsatz und die damit verbundenen Rahmenbedingungen mit allen betroffenen Parteien abzustimmen. Das Ziel, IT-Angriffe abzuwehren, muss im Einklang mit geltenden Datenschutzbestimmungen bleiben. Bei international tätigen Unternehmen kann hier eine Vielzahl nationaler Regelungen zu berücksichtigen sein.

Ausblick

Nach erfolgreicher Einführung eines SIEM Systems lassen sich viele weitere Aspekte einbinden.

In Kombination mit Zeiterfassung und Zugangskontrollsystemen wäre z.B. eine Alarmierung möglich, wenn ein Mitarbeiter sich an seinem Büro-PC einloggt, obwohl er vorher bereits das Gebäude verlassen hat.

Informationen und Events von Gebäudeleittechnik, industriellen Steuerungsanlagen, Alarmanlagen, Zutrittskontrollen oder der Videoüberwachung bieten zusätzliche Möglichkeiten für weitergehende Bewertungsmuster.

Hier wäre ein treffendes Beispiel, wenn ein Mitarbeiter einen Besucher in einem Bereich oder Stockwerk antrifft, wo sich dieser laut Anmeldung nicht aufhalten dürfte. Im zeitlichen Kontext treten nun bestimmte Phänomene an Computern in diesem Bereich auf (die z.B. nur möglich sind, wenn USB-Geräte an das System angeschlossen werden). Eine rein IT-basierte Bewertung würde hier einen wichtigen Teil übersehen, die Berücksichtigung der nicht-IT-basierten Fakten führt hier erst zu einer völlig anderen Bewertung. Hieraus ergibt sich, dass für solche Fälle passende Schnittstellen zur Meldung solcher Vorkommnisse implementiert werden müssen.

Empfehlungen / Fazit

Die aufgeführten Beispiele zeigen einerseits, welchen Vorteil ein solcher Ansatz bietet, andererseits aber auch, welche Aufwände und Kosten entstehen können. Lizenz und Installation sind hier nur ein kleiner Teil. Die laufenden Kosten durch Betreuung, Einbindung zusätzlicher Datenquellen, Anpassen von Regelwerken und vor allem Ausbildung der Mitarbeiter sind nicht zu unterschätzen. Ein zentraler Punkt für den effektiven Einsatz eines SIEM ist eine vollständige Dokumentation aller relevanten Komponenten und eine Beschreibung der IT-relevanten Prozesse. Mit diesen Daten kann dann eine Basislinie definiert werden, sodass bei Abweichungen eine Alarmierung erfolgen kann.

Gezielt eingesetzt und konsequent auf- und ausgebaut liefert es wertvolle Erkenntnisse und verbessert die Reaktionsfähigkeit und Qualität sowie die Bearbeitungszeiten von Vorfällen signifikant.

Die Implementation einer solchen Lösung bis hin zum vollumfänglichen SIEM kann auch in einzelnen Ausbaustufen schrittweise vorgenommen werden.

Viele betriebsrelevanten Probleme und Ausfälle zeichnen sich bereits im Vorfeld ab, werden aber oft in der Vielzahl der Meldungen schlicht nicht erkannt. Hier lohnt sich der toolgestützte Blick in die Logdateien. Schnell erkennt die Administration so Lastspitzen oder Hinweise auf Fehler und kann proaktiv tätig werden, bevor es zu Beeinträchtigungen der Verfügbarkeit von Systemen kommt.

Der vielgerühmte 360° Rundumblick in der IT-Sicherheit erfordert mehr als die rein klassische IT-Sichtweise. Neben den Informationen der typischen Sicherheitssysteme gehören auch jene aus Produktionsanlagen, Gebäudeleittechnik, Zutrittskontrollsystemen u.v.m. dazu.

Für die Integration von Informationen über das Benutzerverhalten müssen von Anfang an organisatorische sowie datenschutzrechtliche Aspekte im Konzept verankert werden.

Frageliste

- Welche kritischen Ressourcen und Prozesse müssen betrachtet werden?
- Welche kritischen Systeme und Übergangspunkte im Netzwerk protokollieren bereits Aktivitäten, Auffälligkeiten und Fehler?
- Welche Erkennungs- und Analyse-Tools werden bereits eingesetzt, die als Datenlieferant dienen können?
- Welche Verfahren für Fehlerbehandlung und Incident Response werden bereits genutzt?
- Welches Datenvolumen und Anzahl an Meldungen werden (schätzungsweise) generiert?
- Welche Informationen müssen für welche Dauer im Zugriff sein oder archiviert werden?
- Welche Regelungen zum Datenschutz müssen getroffen werden?

Christian Schülke ist seit 1988 als Berater für Netzwerk-, Internet- und Informationssicherheit tätig. Er gilt als renommierter Experte bundesweit. Sein Schwerpunkt liegt auf der strategischen Beratung und Konzeption zur Absicherung gegen Cyber-Gefahren und elektronische Wirtschaftsspionage. Gezielt zeigt er Risiken und mögliche Schadensszenarien auf. Durch anschauliche Live-Hacking-Demonstrationen schafft er es, internationale Sicherheitsexperten ebenso wie Unternehmer oder Schüler für die Gefahren aus dem Netz zu sensibilisieren. Nach erfolgten Cyberangriffen und Incidents betreut er Unternehmen bei der Analyse, Auswertung und Aufbereitung der Geschehnisse.
Schülke ist in verschiedenen Expertengruppen sowie als Dozent tätig, verfasst Fachbeiträge und referiert auf Konferenzen sowie internationalen Veranstaltungen. Mehrfach bereits wurde Schülke in Radio und TV interviewt.