RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Alles digital, oder was?
Mittelstand im Umbruch

Cybersicherheit in Zeiten zunehmender Digitalisierung

Trier, 10. September 2019

Verfassungsschutz Rheinland-Pfalz - Cyber Security -

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Verfassungsschutz Rheinland-Pfalz

Abteilung des Ministeriums des Innern und Sport

Guido Jost
IT-Geheimschutzverantwortlicher und IT-Sicherheitsbeauftragter

Beratung und Sensibilisierung im Rahmen des Wirtschaftsschutzes in RP

Thematische Schwerpunkte

- Cyber- und Informationssicherheit
- Stärkung der Wirtschaft gegen Cyber-Risiken
- Cyber Threat Intelligence
- Threat Information Sharing
- Awareness-Maßnahmen

LEBENDIG. SICHER. BÜRGERNAH.

Wir wurden überfallen!

Nein, nicht mit der Pistole in der Hand. Die Verbrecher kamen unbemerkt über eine bis dahin unentdeckte Lücke in unserem Computersystem.

Am 1. Oktober 2018 geschahen unvermittelt seltsame Dinge auf unseren Rechnern. Programme konnten plötzlich nicht mehr gestartet werden, die Telefonanlage „spinnte“.

Was war los? Heute wissen wir, dass über eine unentdeckte Lücke in unserer Firewall ein bis zu dem Zeitpunkt unbekannter Abkömmling eines Virus mit Namen „Dharma“ in unser Netzwerk eingeschleust wurde. Unser Systemadministrator hat nach kurzer Analyse eine Attacke auf unsere IT-Infrastruktur diagnostiziert und um Hilfe gebeten. Auf fast allen Windows-Rechnern im Netz wurden die Dateien auf den lokalen Festplatten verschlüsselt. Unser Produktionsnetz war glücklicherweise nicht betroffen. Dort laufen die Rechner fast alle unter Linux und MacOs.

Wir wurden überfallen!

Was bedeutet das für uns:

1. Das Mailsystem lief unter Exchange, ging nicht mehr
2. Telefonie läuft bei uns übers Netz, ging nicht mehr
2. Löhne auszahlen läuft über eine Bankensoftware, ging nicht mehr
3. Löhne berechnen läuft über ein Lohnprogramm, ging nicht mehr
4. Auftragsbearbeitung und Kalkulation, ging nicht mehr
5. Lieferscheine schreiben, Rechnungen schreiben, ging nicht mehr
6. Anbindung an unsere Logistikpartner DPD, UPS etc. läuft übers Internet, ging nicht mehr.

Wir wurden überfallen!

Kurz gesagt, waren wir lahm gelegt. Die Produktion lief zwar weiter ohne Reibungsverluste, aber der Versand war extrem gefordert. Sämtliche Paketscheine und Speditionsaufträge mussten von Hand geschrieben werden. Das ist bei einigen hundert Sendungen pro Tag schon eine Herausforderung.

Mit der Firma OSS kamen am 02.10.2018 eine Gruppe von IT-Forensikern (ich wusste gar nicht dass der Begriff existiert) zu uns und unterstützte uns in den darauf folgenden Wochen fast rund um die Uhr.

Wir wurden überfallen!

Das Wichtigste war, zunächst das Ausmaß des Schadens einzugrenzen.

Natürlich sichern wir unsere Daten und arbeiten auch mit Cloudsystemen.

Leider fielen die Sicherungen innerhalb des Netzes jedoch dem gleichen Virus zum Opfer. Die letzte saubere Datensicherung unserer kaufmännischen Software war vier Wochen alt und in der Cloud gesichert. Durch die Verschlüsselung der Festplatten wurde hier glücklicherweise die automatische Synchronisation verhindert.
Unsere Finanzbuchhaltung befindet sich schon seit längerer Zeit in der Cloud, die Lohnbuchhaltung sollte zum Jahresende umziehen. Mit Hilfe von D konnten wir den Umzug in die Cloud vorziehen und die alten Daten des Jahres wieder herstellen.

Wir wurden überfallen!

Unsere Unterstützer hatten auf dem verschlüsselten Server eine Nachricht der Verbrecher gefunden. Per Mail nahmen wir Kontakt auf und sahen uns einer Forderung über fast 4.500,-€ zahlbar in Bitcoin gegenüber. Durch Verhandlungen konnten wir den Betrag auf knapp 3.500,- € reduzieren. Nachdem die Erpresser eine Testdatei entschlüsseln konnten, zahlten wir den geforderten Betrag und konnten danach unser Mailsystem mit dem kompletten Archiv zurück entschlüsseln.

Wenn wir die restlichen Dateien (Kaufmännische Software, Lohnbuchhaltung etc.) entschlüsseln wollten, sollten wir weiter Lösegeld zahlen. Auf diese Forderung gingen wir nicht ein. Das Risiko in einer Endlosschleife zu hängen, war uns zu groß.

Wir brachen den Kontakt zu den Verbrechern ab.

Wir wurden überfallen!

Bevor jetzt Fragen kommen: In der Nachricht war nur eine ID, über die wir kommunizierten, wahrscheinlich gehört die ID zu einem ebenfalls gehackten Rechner irgendwo auf diesem Planeten. Den Mailverkehr haben selbstverständlich mit den dazugehörigen Headern an die zuständige Abteilung der Kriminalpolizei übergeben und den Vorgang natürlich auch an die Datenschutzbehörde gemeldet. Wir gehen davon aus, dass keine Daten abgezogen wurden. Der Virus verschlüsselt die Festplatten und lässt keinen Zugriff mehr zu. Mit absoluter Sicherheit können wir das aber nicht bestätigen.

Wir wurden überfallen!

Wir waren am 03.10.2018 immer noch offline, mit erheblichem Einsatz haben die Leute von OSS einen neuen Server auf Linux Basis mit komplett neuer Firewall aufgesetzt. Um wirklich alle Lücken geschlossen zu halten, haben wir eine Anwendung nach der anderen wieder online gebracht. Nur die unbedingt notwendigen Zugänge nach draußen wurden freigegeben. Das bedeutet natürlich immer wieder Verluste, wenn neu installierte Software einfach zu Registrierungszwecken eine Website aufrufen wollte. Das war selbstverständlich zu diesem Zeitpunkt unterbunden. Unser normales Arbeiten während dieser Zeit war extrem erschwert.

Wir wurden überfallen!

Mittlerweile läuft auch wieder alles, fast so wie früher. Dem Engagement unserer Kollegen in der Produktion ist es zu verdanken, dass trotz der Schwierigkeiten keine Sendung verspätet raus ging. Unsere Kunden können das auch bestätigen.

Nachdem fast alle Schäden behoben sind, können wir auch den Umfang beziffern. Uns hat diese Attacke alles in allem ca. 50.000,-€ gekostet. Ein Teil davon sind Update Gebühren für Software, ein Teil Umstellungskosten und Installationskosten und natürlich auch die Kosten für das Unterstützerteam um DK und AB. Die Jungs haben großartige Arbeit geleistet, teilweise rund um die Uhr gearbeitet, waren am Feiertag und am Wochenende im Einsatz.

Wir wurden überfallen!

In der Rückschau ist für uns das Ärgerliche, dass wir uns sicher wähnten und doch nicht sicher waren. Datenschutz und Datensicherung hat bei uns einen hohen Stellenwert. Das war auch der Grund, warum wir schon im letzten Jahr unsere Finanzbuchhaltung zu Datev in die Cloud umgezogen haben und zu diesem Jahreswechsel mit der Lohnbuchhaltung folgen wollten. Wir gehen davon aus, dass ein Konzern wie Dt wesentlich mehr Ressourcen zur Verfügung hat als ein Unternehmen wie B&K. Wir haben auch unsere Mitarbeiter geschult im Hinblick auf Phishing Mails und dem Erkennen von Malware. Letztlich zeigt die Attacke aber, dass wir selbst immer wieder nach möglichen Lücken und Schwachstellen suchen müssen. Dass auch Weltkonzerne wie Facebook (im September 2018) oder die Telekom (November 2016) Opfer von Cyberkriminalität geworden sind, ist uns dabei auch kein Trost.

Wir wurden überfallen!

Warum schreiben wir hier darüber? Warum haben wir mit dem Saarländischen Rundfunk geredet und die Sache nicht einfach unter den Teppich gekehrt? Das ist auch laut Spiegel Online das übliche Vorgehen. Dabei entstehen alleine in Deutschland durch die Cyberkriminalität jährlich Schäden von über 40 Milliarden €.

Wir haben aus diesem Angriff gelernt, wir möchten diese Erfahrungen weitergeben und mit helfen ein Bewusstsein für dieses Thema zu wecken. Jeder vernünftige Unternehmer achtet in seinem Unternehmen auf Arbeitsschutz und die Abwehr von alltäglichen Gefahren. Diese Cyberkriminalität ist eine häufig unterschätzte, weil unsichtbare Gefahr, die aber dafür um so realer ist.

Wir wurden überfallen!

Wer nun denkt, welcher Hacker interessiert sich schon für mein Unternehmen, dem sei gesagt, genau das ist der Punkt, die Hacker interessieren sich nicht für das Unternehmen, kennen dieses normalerweise gar nicht mal. Die Schadprogramme laufen als „Roboter“ über das weltweite Netz und suchen ständig nach irgendwelchen Schwachstellen. Sobald eine gefunden ist, erfolgt automatisch die Attacke.

https://www.braun-klein.de/wir-wurden-ueberfallen/

Wie ein Cyberangriff das Unternehmen lähmte

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

STUTTGARTER-ZEITUNG.DE

Elektrowerkzeughersteller Metabo aus Nürtingen

Wie ein Cyberangriff das Unternehmen lähmte

Von Florian Gann - 17. Juli 2018 - 18:48 Uhr

Ein IT-Experte des Werkzeugherstellers Metabo aus Nürtingen berichtet, wie eine Cyberattacke das Unternehmen getroffen hat – und wie die Mitarbeiter damit umgegangen sind.

Ein Cyberangriff legte Metabo 2017 für mehrere Tage lahm. Foto:dpa Foto: dpa

Stuttgart - Von den ersten Auffälligkeiten bis zur Erpressernachricht vergingen nur wenige Minuten. Der 27. Juni 2017 ist Thomas Rinas noch gut in Erinnerung. Der IT-Leiter des Nürtinger Elektrowerkzeugherstellers Metabo musste in kürzester Zeit entscheiden, wie es nach einer Cyberattacke weitergeht – zu einem Zeitpunkt, da er selbst noch nicht so genau wusste, was überhaupt vorgefallen war. „Wir wussten zunächst nicht einmal, welche IT-Systeme wir überhaupt retten können“, sagt Rinas. Man entschied sich, vorerst den Stecker zu ziehen.

LEBENDIG. SICHER. BÜRGERNAH.

Wie ein Cyberangriff das Unternehmen lähmte

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Cyberdesaster durch Buchhaltungssoftware

Der Cyberangriff ging von einem Programm aus, das Metabo in der Buchhaltung verwendete. Im Team des Softwareherstellers saß ein Hacker, der einen Trojaner programmiert hatte. Die auch Ransomware genannten Schadprogramme verschlüsseln eigene Daten – um Unternehmen zu schädigen oder Lösegeld zu erpressen. Mit einem Update der Buchhaltungssoftware landete das Schadprogramm im Computernetzwerk des Nürtinger Unternehmens – ein Kollateralschaden, denn gegolten hatte der mutmaßlich von Russland lancierte Not-Petya-Angriff eigentlich der Ukraine. Weil dort dieselbe Software wie bei Metabo eingesetzt wird, traf es auch die Werkzeugbauer als eines der ersten Unternehmen in Deutschland.

Den Stecker ziehen, das bedeutete laut Rinas: „Man wird in die Steinzeit zurückgebombt." E-Mail, Netzwerk, Telefone – nichts ging mehr. Eine Krisen-Mail-Adresse richtete die IT bei einem Netzanbieter ein, Mitarbeiter mussten Festplatten von einem Elektronikmarkt organisieren und hatten mehr als 1000 Rechner neu einzurichten. „Turnschuhinformatik" nennt Rinas die mit viel Gerenne verbundenen Aufgaben. In der Zwischenzeit stand die Produktion längst still, und die Auslieferung war blockiert. Rund um den IT-Leiter entstand ein Krisenmanagement, das sich vor allem mit Stift und Papier organisierte. „Ein analoges Verfahren rettete die digitale Welt", fasst Rinas die Erfahrung zusammen.

LEBENDIG. SICHER. BÜRGERNAH.

Wie ein Cyberangriff das Unternehmen lähmte

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Es dauert Tage, bis der Betrieb wieder läuft

Nach fünf Tagen sind erste Teilbereiche des Unternehmens wieder einsatzbereit, nach neun Tagen laufen wieder Bohrmaschinen und Kreissägen vom Band. „Der größte Erfolgsfaktor war der Spirit", meint Rinas. Alle Mitarbeiter hätten mitangepackt, nicht nur die Informatik. Weniger gut ist der IT-Manager jedoch auf die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu sprechen. Alles, was er von dem Amt gewollt hätte, sei eine Adresse gewesen, an die er sich wenden kann, sagt Rinas: „Ohne Erfolg."

Als Konsequenz aus dem Erlebten haben die Informatiker von Metabo diverse Vorsichtsmaßnahmen getroffen. Mittlerweile müssten die Administrator-Zugänge eigens bestellt werden und würden nach einer gewissen Zeit wieder ablaufen. Auch bei den im Unternehmen verwendeten Programmen habe man aufgeräumt, erklärt Rinas weiter. Aber fühlt er sich jetzt sicher vor weiteren Angriffen? Die Angriffsarten, die er schon kenne, machten ihm keine Sorgen mehr, sagt Rinas. Und relativiert: „Was wir erlebt haben, war eine ungezielte Attacke. Wenn jemand einen gezielten Angriff startet, ist die Abwehr mit ziemlicher Sicherheit noch schwieriger." Diese Cyberattacken seien aus Sicht der Täter wohl besonders effizient: „Man kann aus der Deckung heraus arbeiten und die eigenen Spuren so verwischen, so dass man nur ein geringes Risiko eingeht, erwischt zu werden."

LEBENDIG. SICHER. BÜRGERNAH.

Wie ein Cyberangriff das Unternehmen lähmte

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

„Attacken abzuwehren wird immer schwerer“

Für mittelgroße Unternehmen wie Metabo ist das Thema Cybersicherheit eine besondere Herausforderung. In den Jahren 2009 und 2010 stand Metabo vorübergehend vor dem Aus. Man musste aufgrund des Spardrucks einen Mittelweg bei der IT-Sicherheit finden. Mit dem Sicherheitsrisiko der Gegenwart sind Unternehmen wie der Werkzeughersteller stark gefordert: „Wir wurden durch diese bislang unbekannte Form der digitalen Attacke ohne jede Vorwarnung in die vorderste Front der Cyberkriminalität katapultiert“, sagt Rinas. Was bedeutet das für die Zukunft? „Mit der Digitalisierung wächst die Komplexität weiter, und es wird immer schwieriger für Unternehmen, alle Attacken abzuwehren“, schätzt Rinas die Situation ein.

LEBENDIG. SICHER. BÜRGERNAH.

Automatisierte Cyber-Angriffe durch Spear-Phishing

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Cyber-Attacke lähmt Krauss Maffei: Kommen die Hacker aus Nordkorea oder Russland?

Aktualisiert: 04.01.19 - 09:31

www.tz.de

LEBENDIG. SICHER. BÜRGERNAH.

Automatisierte Cyber-Angriffe durch Spear-Phishing

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Der Münchner Mittelständler Krauss Maffei ist Opfer eines massiven Cyber-Angriffs geworden. Im Verdacht stehen sowohl nordkoreanische wie auch russische Hacker.

München – Der Münchner Maschinenbauer Krauss Maffei kämpft seit mehreren Wochen mit den Folgen eines Hackerangriffs. Die Angreifer hätten mittlerweile auch Lösegeld gefordert, bestätigte Firmensprecher Uli Pecher. Ob das 2016 von chinesischen Investoren übernommene Unternehmen gezahlt hat, sagte er nicht.

Hauptziel des Angriffs sei die Münchner Zentrale gewesen, wo die Produktion immer noch beeinträchtigt ist. Auch einige kleinere Standorte bundesweit seien betroffen gewesen, nicht jedoch weitere große Fertigungen in Hannover, der Schweiz und den USA. Stillschweigen herrscht auch hinsichtlich Schadensumfängen oder den Ursprüngen des Angriffs. Auch mit Hilfe externer IT-Forensiker untersuchen bei Krauss Maffei derzeit drei Expertenteams unter anderem, ob ein unter dem Namen Emotet seit 2014 in der Szene bekannter Trojaner dafür gesorgt hat, dass der Maschinenbauer am 21. November am Zentralstandort München-Allach mit seinen 1800 Beschäftigten alle IT-System herunterfahren musste. Emotet verbreitet sich über geöffnete E-Mail-Anhänge. Inzwischen sei man auf dem „Weg zum Normalzustand", die Fertigung werde hochgefahren. Wichtige Dateien würden zum Laufen gebracht.

LEBENDIG. SICHER. BÜRGERNAH.

Automatisierte Cyber-Angriffe durch Spear-Phishing

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Durch das sogenannte "Outlook-Harvesting" ist Emotet in der Lage, authentisch aussehende Spam-Mails zu verschicken. Dazu liest die Schadsoftware Kontaktbeziehungen und seit einigen Wochen auch E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms in nachfolgenden Spam-Kampagnen, so dass die Empfänger fingierte Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen. Das BSI rechnet daher künftig mit einer weiteren Zunahme an gut gemachten, automatisierten Social-Engineering-Angriffen dieser Art, die für die Empfänger kaum noch als solche zu identifizieren sind. Diese Methode eignet sich ebenfalls zum Einsatz von hochspezialisierten Spear-Phishing-Angriffen auf besonders hochwertige Ziele.

Emotet verfügt zudem über die Möglichkeit, weitere Schadsoftware nachzuladen, sobald es einen Computer infiziert hat. Diese Schadprogramme ermöglichen den Angreifern etwa das Auslesen von Zugangsdaten und vollständigen Remote-Zugriff auf das System. Zuletzt wurde insbesondere der Banking-Trojaner "Trickbot" nachgeladen, der sich u.a. über das Auslesen von Zugangsdaten (Mimikatz) und SMB-Schwachstellen (Eternal Blue/Romance) selbstständig in einem Netzwerk ausbreiten kann. Je nach Netzwerkkonfiguration ist es dabei zu Ausfällen kompletter Unternehmensnetzwerke gekommen. Die Schadprogramme werden aufgrund ständiger Modifikationen zunächst meist nicht von gängigen Virenschutzprogrammen erkannt und nehmen tiefgreifende Änderungen an infizierten Systemen vor.

LEBENDIG. SICHER. BÜRGERNAH.

Cyber-Angriffskampagne “Berserk Bear”

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Angriffe und Aufklärungsaktivitäten die der Hackergruppe Berserk Bear (Wütender Bär) zugerechnet werden, sind bereits seit 2011 bekannt.

Im aktuellen Zielspektrum der Angreifer liegen vorwiegend KRITIS-Unternehmen (z.B. Energieversorgung, Wasserversorgung /-entsorgung, Informationstechnik/Telekommunikation).

Die Angreifer verwenden vielfach öffentlich zugängliche Angriffswerkzeuge und versuchen unzureichend gesicherte Systeme über unterschiedliche Angriffsvektoren unter ihre Kontrolle zu bringen.

LEBENDIG. SICHER. BÜRGERNAH.

Cyber-Angriffskampagne “Berserk Bear”

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Die Hackergruppe Berserk Bear wird dem russischen Inlandsgeheimdienst FSB zugerechnet, der jedoch auch Auslandsaufklärung und Spionageaktivitäten betreibt.

Die Kampagne stellt derzeit eine der aktivsten und aggressivsten Cyberspionageoperationen im virtuellen Raum dar.

Aufgrund einer Cyber-Kampagne im Jahre 2017, von der u.a. auch der Internet-Anbieter Netcom BW (Tochterunternehmen des Energieversorgers EnBW) betroffen war, wurde seitens der Generalbundesanwaltschaft ein Ermittlungsverfahren eingeleitet und hat das LKA BW mit den Ermittlungen betraut.

LEBENDIG. SICHER. BÜRGERNAH.

Cyber-Angriffskampagne “Berserk Bear”

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Schwachstellen in der Router-Software des Herstellers Cisco.

Von den Angriffen sind bisher weltweit mind. 26.000 CISCO Router betroffen, die das Netzprotokoll **Generic Routing Encapsulation (GRE)**, ein Netzprotokoll, welches dazu dient, andere Protokolle einzukapseln und getunnelt über das Internet Protocol (IP) zu transportieren. **Ciscos Smart Install (SMI),** mit dem Geräte aus der Ferne konfiguriert werden können, oder das **Simple Network Management Protocol (SNMP)**, das der zentralen Steuerung und Überwachung von Netzwerkgeräten dient, nutzen.

LEBENDIG. SICHER. BÜRGERNAH.

Cyber-Angriffskampagne “Berserk Bear”

Das Server Message Block (SMB) -Protokoll dient als Client/Server-Protokoll für die Freigabe von Netzwerkdateien und ermöglicht es Anwendungen, auf einem Client Dateien zu lesen, in Dateien zu schreiben sowie Dienste von Serverprogrammen in einem Computernetzwerk anzufordern.

Es empfiehlt sich, die Kommunikation aller SMB-Varianten nach außen mit dem Internet zu unterbinden.

Dies geschieht dadurch, dass der TCP-Port 445, die UDP-Ports 137-138 und der TCP-Port 139 nicht von außen zugänglich sind.

UNC-Verweis auf eine vom Angreifer kontrollierte, Windows-Dateifreigabe enthalten

Cyber-Angriffskampagne “Berserk Bear”

Als weiteren Angriffsvektor verwendet die Angreifer-Gruppe Spear Phishing Mails mit maliziösen Anhängen oder vom Angreifer veränderte Webseiten (Watering-Hole-Angriffe).

Angry IP Scanner	Offener Netzwerk-Scanner
Backdoor.goodor	Backdoor
Dorshell	Backdoor
Get-GPPPassword	PowerShell script
Inveigh	Spoofing und man-in-the-middle tool
Malicious JavaScript downloader	JavaScript Downloader
Malicious Shortcut File	Windows shortcut file (remote fileserver)
Malicious Word document	Maliziöses Word document
Mimikatz	Password extraction
Phishery	spear-phishing framework
Powershell	
Psexec	Remote command tool
RDP Bruteforcer	RDP brute forcing tool
Screenutil	capture screenshots
Z_Webshell	ASPX web-shell
Heriplor	Backdoor

Hot Topics
Identifizierung der „Kronjuwelen“

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Sie können nicht alle Informationen und Werte Ihres Unternehmens in gleichem Maße schützen. Priorisieren Sie.

Konzentrieren Sie sich auf Ihre wesentlichsten **Informations**werte im Unternehmen!

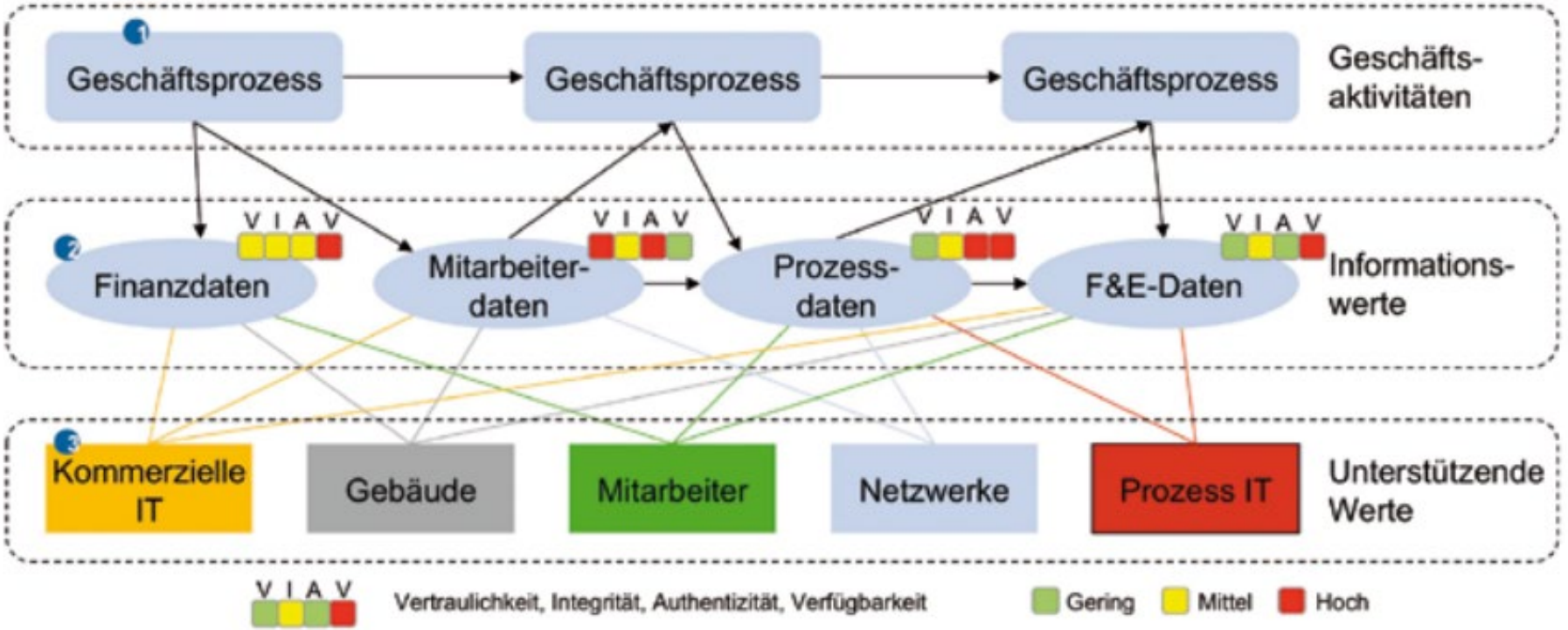
Kerngeschäftsprozesse und notwendige Unterstützungsprozesse sollten identifiziert werden
Kritische Infrastrukturen für Ihr Unternehmen sollten bekannt sein.
Sensible und unternehmenskritische Daten und Informationen sollten festgelegt sein.

Entsprechende Sicherheitsmaßnahmen sind dann festzulegen, zu priorisieren und umzusetzen.

LEBENDIG. SICHER. BÜRGERNAH.

Modellierung der Informationsverarbeitung

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT



www.kes.info

LEBENDIG. SICHER. BÜRGERNAH.

Einst Science-Fiction, heute Realität

Press Release

Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says

Jenalea Howell | October 24, 2017

Quelle: ihs.com

Klassisches Security-Information- und Event-Management-System Reporting

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

SIEM Unique Events

Event Name	Total #	Unique Src #	Unique Dst #
POLICY PE EXE or DLL Windows file download"	137328	669	8
INFO JAVA - ClassID"	17350	59	8
SCAN NMAP -sS window 1024"	10423	2068	176
INFO EXE IsDebuggerPresent (Used in Malware	7147	94	7
INFO EXE - Served Attached HTTP"	6182	32	7
L SHELLCODE x86 inc ebx NOOP"	5803	14	8
USER_AGENTS Suspicious Mozilla User-Agent (Mozilla/5.0)"	5595	71	37
SCAN Behavioral Unusual Port 1433 traffic, Potential	4816	8	8
SHELLCODE Possible Call with No Offset TCP	4200	73	9
SCAN Potential SSH Scan"	3218	94	6
WEB_CLIENT Hex Obfuscation of document.write %	2706	42	6
USER_AGENTS BLEXBot User-Agent"	2175	26	22
SCAN SSH BruteForce Tool with fake PUTTY version"	1889	21	1

LEBENDIG. SICHER. BÜRGERNAH.

Der klassische Perimeter-Schutz ist unzureichend

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Mit einer vernünftigen Firewall, aktuellem Spam- und Virenschutz sollte mein Unternehmen doch ausreichend gegen Cyberbedrohungen geschützt sein, oder?! Eine folgenschwere Fehleinschätzung.

LEBENDIG. SICHER. BÜRGERNAH.

Der klassische Perimeter-Schutz ist unzureichend

Hacker haben zudem oft den Vorteil, dass Unternehmen den größten Teil ihrer Cybersicherheitsressourcen in die Verteidigung ihrer Netzwerkgrenzen (Perimeterschutz) stecken.

Für fast alle Cyber-Angriffe der jüngsten Vergangenheit gilt: Der Perimeter-Schutz wird erfolgreich umgangen und privilegierte Benutzerkonten werden als Einfallstor genutzt.

Es stellt sich nicht mehr die Frage, ob ein Angriff geschehen wird, sondern vielmehr wann er passiert. Aus diesem Grund müssen Unternehmen sich von einer traditionellen, auf das Netzwerkperimeter zentrierten Sicherheitsstrategie verabschieden und stattdessen den Ernstfall absichern.

Der klassische Perimeter-Schutz ist unzureichend

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Die heutigen Cybersicherheitseinrichtungen weisen einige gemeinsame Probleme auf: riesige Datenvolumina, fehlende Analytiker und immer komplexer werdende Angriffe. Die aktuellen Sicherheitsinfrastrukturen bieten zahlreiche Tools zur Verwaltung dieser Informationen, jedoch wenig Integration zwischen ihnen.

Dies bedeutet einen erheblichen Entwicklungsaufwand für die Verwaltung von Systemen und eine unvermeidliche Vergeudung von ohnehin schon begrenzten Ressourcen und Zeit.

LEBENDIG. SICHER. BÜRGERNAH.

Frühzeitige Erkennung von Angriffen

Die frühzeitige Erkennung von Bedrohungen bietet einen doppelten Vorteil:

Zum einen werden Risiken minimiert, da Angriffe abgewehrt werden, bevor sie Schaden anrichten können, zum anderen werden hierdurch Folgewarnungen, die an späterer Stelle im Angriffszyklus entstehen würden, eliminiert, wodurch die Kosten für die Analyse sinken.

Frühzeitige Erkennung von Angriffen

Ein großer Teil der Daten die benötigt werden um ein verlässliches Bild der aktuellen Sicherheitslage zu erhalten, findet sich direkt in jeder Organisation. Seien es Informationen aus Application Logs, Systemen zur Intrusion Detection und Intrusion Prevention, Firewalls, Endpoint-Antivirus-Lösungen und anderen Sicherheitsmaßnahmen.
Aus ihnen lassen sich bereits viele Informationen darüber gewinnen, was im Firmennetz vorgeht und welche Schwachstellen und Gefahrenpunkte vorhanden sind.

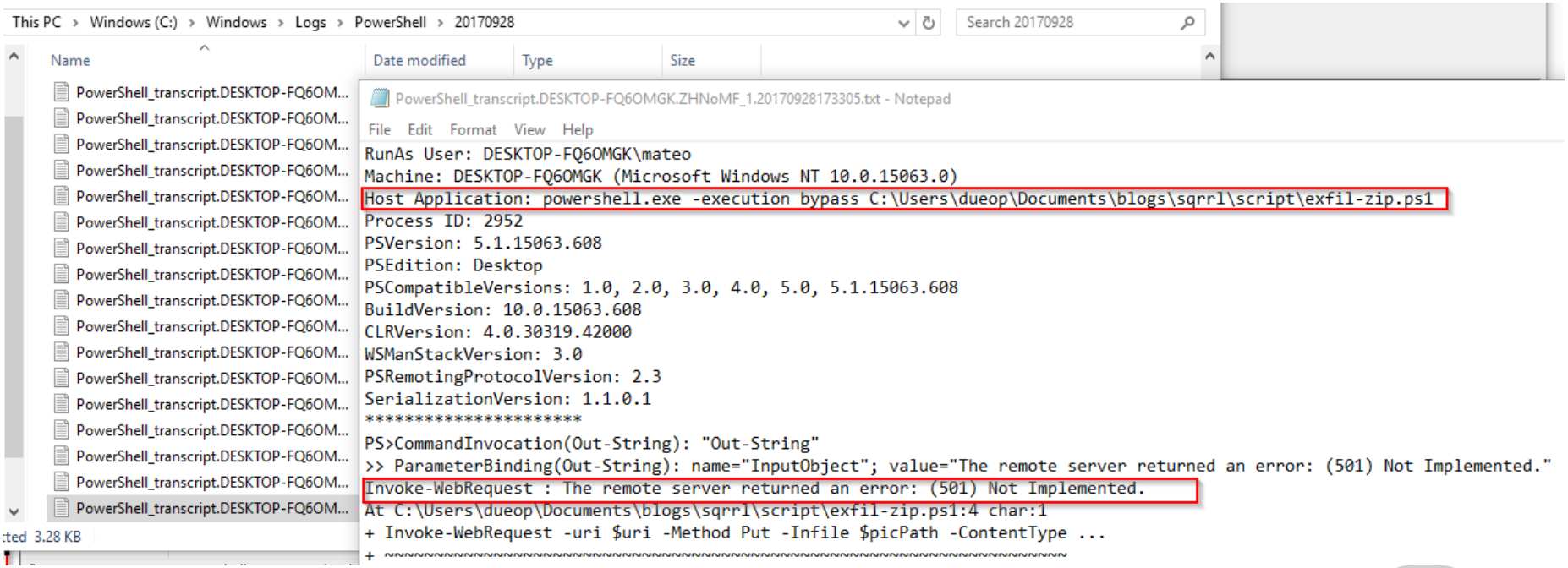
Ein großes Problem stellt oftmals die Heterogenität der Datenstrukturen dar.
Weitere Datenquellen sind bspw.:

Cyber Threat Intelligence Indikatoren

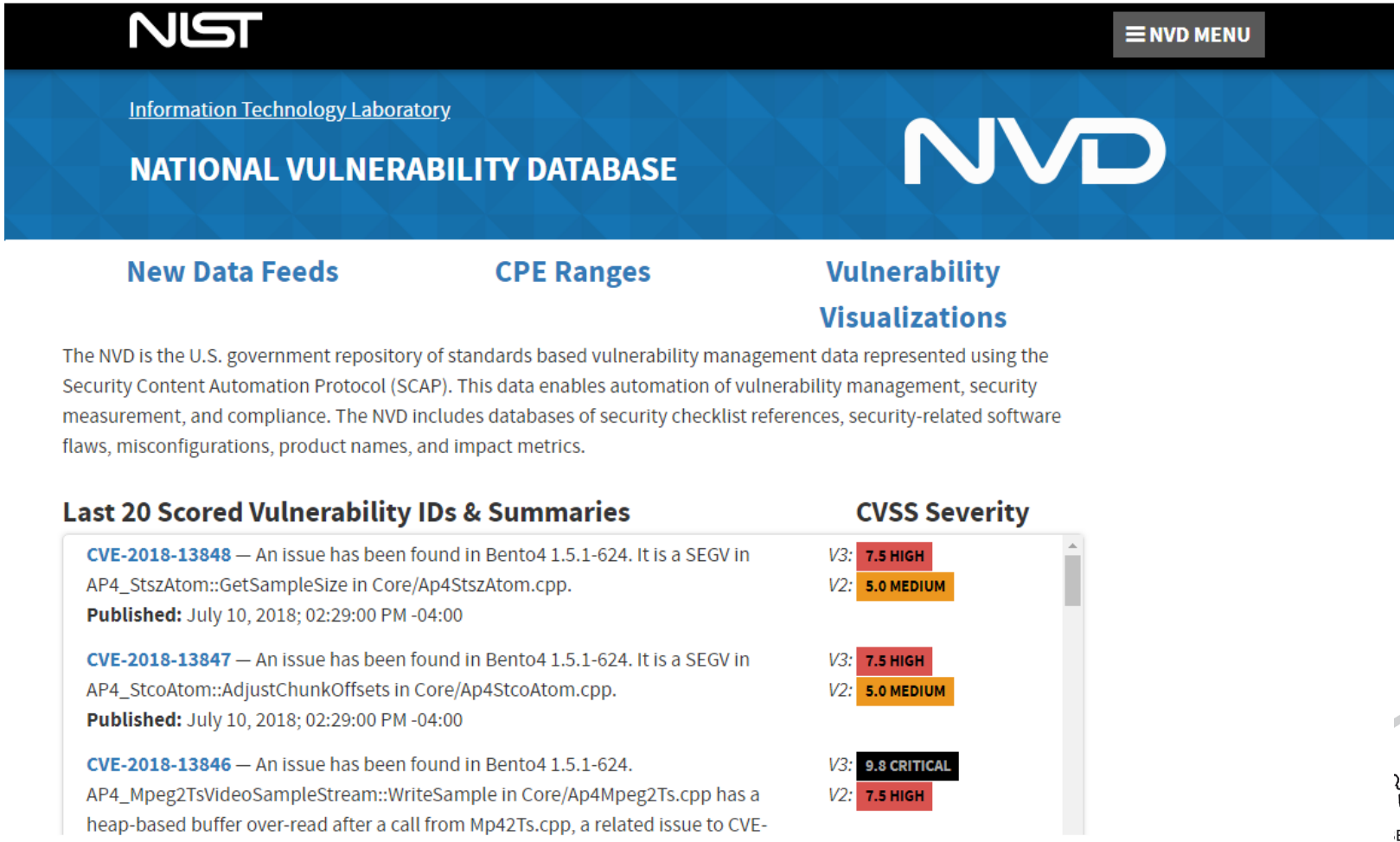
3/23/2012 1:33:02 PM	Adding logical item: SQL (SQL:\)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Default Instance (SQL:\Default Instance)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: SQL Server Folders (SQL:\Default Instance\SQL Server Folders)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Databases (SQL:\Default Instance\Databases)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Default Database Path (Data) (SQL:\Default Instance\SQL Server Fold...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Default Database Path (Log) (SQL:\Default Instance\SQL Server Folder...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Backup Directory (SQL:\Default Instance\SQL Server Folders\Backup D...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: SQL Server Log Path (SQL:\Default Instance\SQL Server Folders\SQL...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Full-Text Catalog Path (SQL:\Default Instance\SQL Server Folders\Full-...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Jobs Working Directory (SQL:\Default Instance\SQL Server Folders\Jo...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: Replication Tasks Path (SQL:\Default Instance\SQL Server Folders\Rep...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: System Databases (SQL:\Default Instance\Databases\System Databas...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: User Databases (SQL:\Default Instance\Databases\User Databases)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: db1 (SQL:\Default Instance\Databases\User Databases\db1)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: master (SQL:\Default Instance\Databases\System Databases\master)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: model (SQL:\Default Instance\Databases\System Databases\model)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: msdb (SQL:\Default Instance\Databases\System Databases\msdb)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: ReportServer (SQL:\Default Instance\Databases\User Databases\Repo...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: ReportServerTempDB (SQL:\Default Instance\Databases\User Databas...	Management Service
3/23/2012 1:33:02 PM	Adding logical item: tempdb (SQL:\Default Instance\Databases\System Databases\tempdb)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: C: (C:\)	Management Service
3/23/2012 1:33:02 PM	Adding logical item: D: (D:\)	Management Service
3/23/2012 1:33:03 PM	Adding logical item: C: (C:\)	Management Service
3/23/2012 1:33:03 PM	Adding logical item: D: (D:\)	Management Service
3/23/2012 1:33:03 PM	Workload Apply Defaults	Management Service
3/23/2012 1:33:03 PM	Adding logical item: Hyper-V Virtual Machine (Vm:\)	Management Service
3/23/2012 1:33:03 PM	System.Management.ManagementException: Invalid namespace at System.Managem...	Management Service
3/23/2012 1:33:12 PM	GetFilesCommand for 'C:\' returned 16 items	Management Service
3/23/2012 1:33:13 PM	GetFilesCommand for 'C:\BgInfo\' returned 3 items	Management Service
3/23/2012 1:34:06 PM	Connection request from IP address 192.168.1.6	Double-Take
3/23/2012 1:34:06 PM	Connection from 192.168.1.6:6320 is a server to server connection.	Double-Take
3/23/2012 1:34:19 PM	Adding Connection: Id = 2a96a7c2-a75c-4c47-8e49-4ebbac450f1b, ReplicationSetName =...	Management Service
3/23/2012 1:34:19 PM	RepSet Modified: FilesAndFolders_7d16d34a3c09467eaf42efdfb5279833	Double-Take

NDIG. SICHER.
BÜRGERNAH.

Cyber Threat Intelligence Indikatoren



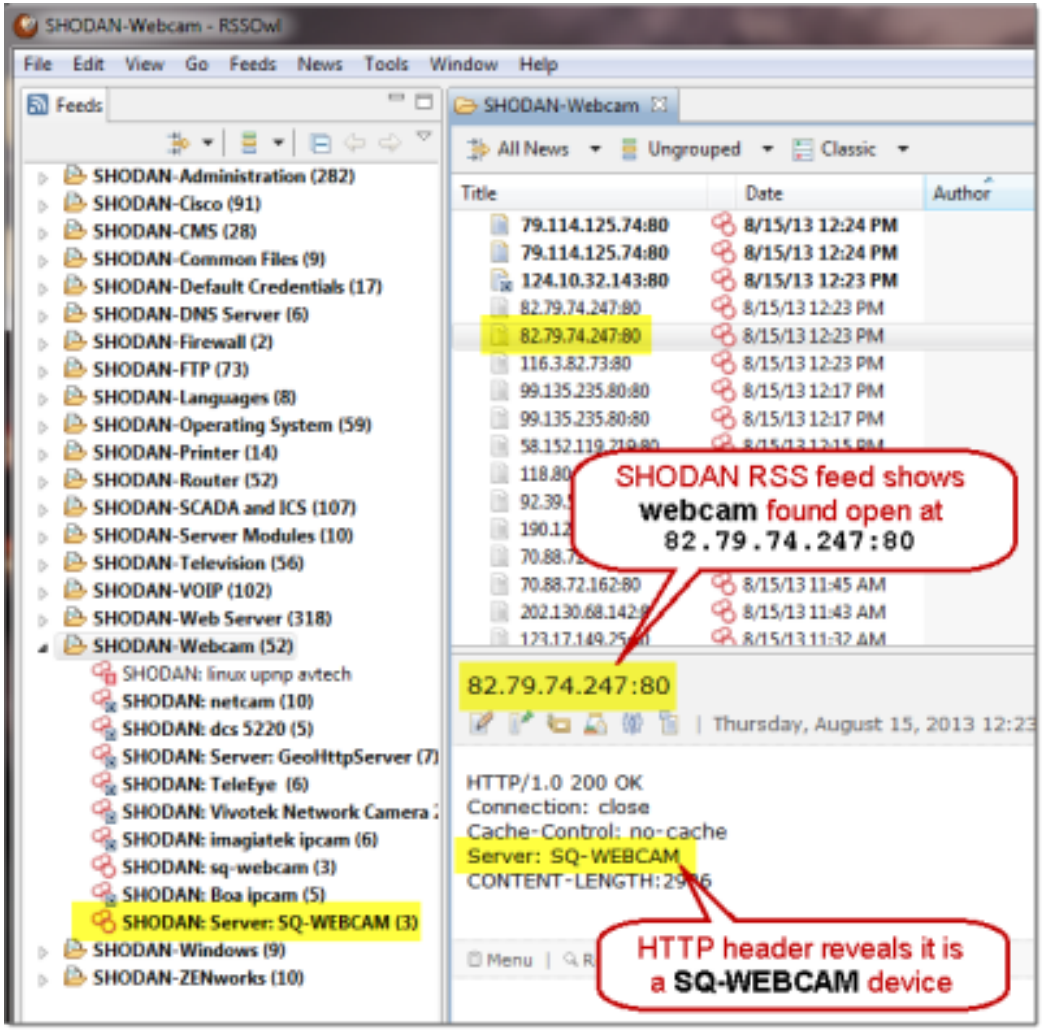
Cyber Threat Intelligence Indikatoren



Cyber Threat Intelligence Indikatoren

e4561c7bfc7ce3a25b8448bf7945b63c	http://cs-czosnusie.cba.pl/jkYTFhb7?PXbuYowwW=zQHgMYXfmlf
e4561c7bfc7ce3a25b8448bf7945b63c	http://sulportale.50webs.com/jkYTFhb7?PXbuYowwW=zQHgMYXfmlf
cb5c4ca780bb78ae5ee41aa944d97703	http://concurs.kzh.hi2.ro/jkYTFhb7?tBRRkEdyVnF=WTiyfMkoomp
cb5c4ca780bb78ae5ee41aa944d97703	http://edios.vzpsoft.com/jkYTFhb7?tBRRkEdyVnF=WTiyfMkoomp
cb5c4ca780bb78ae5ee41aa944d97703	http://www.kdr.easynet.co.uk/jkYTFhb7?tBRRkEdyVnF=WTiyfMkoomp
6cc87c04f193b71a385a9d9f166b2c22	http://rgcgifuhashima.aikotoba.jp/jkYTFhb7?dOPpNG=NXoNiy
3e3bf4d2ca6b70a4e416a14dcc6d1186	http://sulportale.50webs.com/jkYTFhb7?tVEczs=vxHzINWgR

Cyber Threat Intelligence Indikatoren



Cyber Threat Intelligence Indikatoren

Fazit und Ausblick

Der Schutz der IT-Infrastruktur vor Angriffen stellt eine permanente Herausforderung dar und ist oft ein Wettlauf mit den Angreifern.

In der Praxis bedeutet dies, das klassische Schutzmechanismen wie Firewall, Antivirus oder andere Endpunkt-basierte Sicherheitstools an ihre Grenzen stoßen und alleine nicht mehr ausreichend sind.
Die enormen Mengen an sicherheitsrelevanten Daten erfordern neue IT-Sicherheits-Analyse-Tools, damit IT-Sicherheitsverantwortliche schnell und zuverlässig gefährlichen Code oder ein abnormales Verhalten im Netzwerk und/oder Rechenzentrum aufspüren können.

Vielen Dank für Ihre Aufmerksamkeit

Guido Jost
IT-Geheimschutzverantwortlicher

Ministerium des Innern und für Sport

guido.jost@mdi.rlp.de