

MONTHLY SECURITY SUMMARY



AUSGABE JANUAR 2023

OPENAI CHATGPT UND MICROSOFT INTUNE

CHATGPT ALS NEUER SPIELGEFÄHRTE

Durch die neueste Generation von Chatbots wird es möglich, hochkomplexe Probleme zu diskutieren. Wir zeigen, welche Möglichkeiten gegeben sind und welche Limitierungen bestehen.

DEFENDER-CONFIGS MIT INTUNE ANALYSIEREN

Microsoft Intune macht das Analysieren von Einstellungen relativ komplex. Wir zeigen auf, wie dennoch konkrete und verlässliche Analysen möglich sind.



Januar 2023: Bitte keine dystopische KI

Künstliche Intelligenz ist ein Thema, das immer mehr in den Fokus rückt und das Potenzial hat, unser Leben in vielerlei Hinsicht zu verbessern. Von der Automatisierung von Routineaufgaben bis hin zur Lösung komplexer Probleme in Wissenschaft und Medizin - die Möglichkeiten sind nahezu unbegrenzt.

Doch mit dem Fortschritt der Technologie kommen auch Bedenken auf. KI kann menschliche Arbeitsplätze ersetzen, ethische und moralische Fragen aufwerfen. Es ist unabdingbar, dass wir uns diesen Herausforderungen stellen und gewährleisten, dass der Einsatz von KI fair und verantwortungsvoll erfolgt.

Vor allem muss verhindert werden, dass *Big Tech Companies* ihre Vorherrschaft ausbauen und zementieren können. Denn dadurch würde sich die Macht nachhaltig vom Staat zu einigen wenigen Firmen verschieben. Ein dystopisches Szenario, vor dem uns Science-Fiction Bücher und Filme seit Jahrzehnten warnen.

Insgesamt ist KI ein mächtiges Werkzeug mit unglaublichem Potenzial, aber es ist wichtig, dass wir es mit Sorgfalt und Verantwortung einsetzen. Deshalb ist es zentral, dass die Entwicklung von KI von einer Vielfalt von Perspektiven und Stimmen geleitet wird. Wenn wir dies tun, kann KI uns helfen, eine bessere Zukunft für alle zu schaffen.

Marc Ruef
Head of Research



NEWS

WAS IST BEI UNS PASSIERT?**INTERVIEW IN FERNSEHDOKUMENTATION ÜBER CYBERCRIME**

In der DOK-Sendung *Cyber Crime & Darknet – Von Liebesschwindel, Drogengeschäften und Pädophilie* wurde sich mit verschiedenen Aspekten der Computerkriminalität auseinandergesetzt. In Bezug auf das *Darknet* kommt Marc Ruef zu Wort, der die Grundzüge des wirtschaftlich motivierten Untergrunds im Internet skizziert. Dabei wird mitunter ebenfalls darauf eingegangen, dass viele Angebote Fakes und Scam sind.

VORTRAG AN KARLSRUHER INSTITUT FÜR TECHNOLOGIE

Am 16. Januar hielt Marisa Tschopp einen Vortrag im Rahmen des Forschungsprogramms der *KD²School* an der *Fakultät für Wirtschaftswissenschaften* des *Karlsruher Institut für Technologie*. Die Forschungsgruppe *Marketing & Vertrieb* ist Teil eines öffentlich geförderten und koordinierten Programms und erschliesst ein Themenfeld, das derzeit vor allem mit gewinnorientierten oder politischen Zielen erforscht wird.

INTERVIEW ZU KÜNSTLICHER INTELLIGENZ IN DER PSYCHOLOGIE

Künstliche Intelligenz hält Einzug in verschiedene Fachbereiche. Hierbei hat grad *ChatGPT* aufgezeigt, wie mächtig und disruptiv gewisse Lösungen sein können. Für *t3n* hat sich Marisa Tschopp mit dem Journalisten Matthias Kreienbrink zusammengesetzt und diskutiert, inwiefern hier Veränderungen im Bereich *Psychotherapie* zu erwarten sind.

SCIP BUCHREIHE

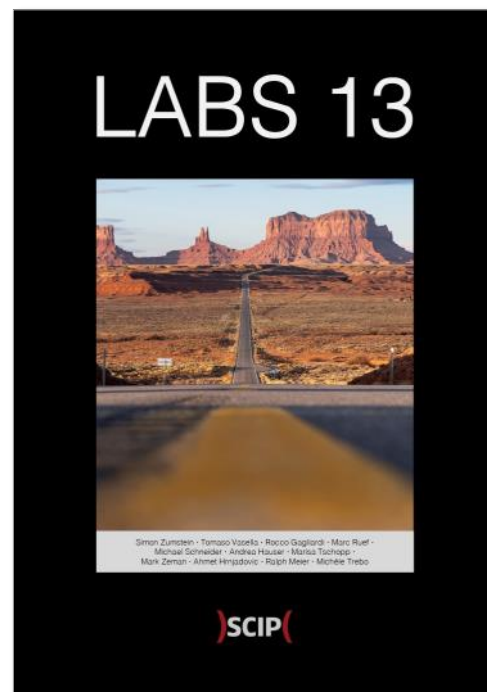
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf [unserer Webseite](#).



ISBN 978-3-907109-30-4 [de]

ISBN 978-3-907109-31-1 [en]

AGIERE STETS AUS DEM VERBORGENEN

ROCCO GAGLIARDI

CHATGPT ALS NEUER SPIELGEFÄHRTE

Dieser Artikel wurde Anfang Januar 2023 veröffentlicht, aber die Idee und die Ausarbeitung begannen am 3. Dezember 2022. Zwei Tage sind vergangen, seit Sam Altman die Veröffentlichung von ChatGPT angekündigt hat, und meine Twitter-Timeline ist voll mit #ChatGPT getaggten Tweets. Nachdem ich ein paar Stunden mit dem Bot gespielt hatte, war klar, dass die Interaktion mit einem ähnlichen Tool nicht nur unterhaltsam, sondern auch nützlich ist und mit den nächsten Versionen unverzichtbar werden wird.

ChatGPT ist ein Chatbot, der auf der Technologie OpenAI's GPT-3.5 basiert. Auf die Frage nach seiner Quintessenz antwortet der Bot:

As a large language model trained by OpenAI, I use machine learning algorithms and a massive dataset of text to generate responses to questions and provide information on a wide range of topics [...] including general knowledge, current events, history, science, technology, and many other subjects. I am not an expert on any specific topic, but I am able to provide information and answer questions based on my pre-existing knowledge. [...] I can only provide

information based on the text that I have been trained on, which has a knowledge cutoff of 2021.

Wenn Sie den Bot nach Was ist ChatGPT fragen, lautet die Antwort, dass er mit einer Technologie namens ChatGPT nicht vertraut ist. Wahrscheinlich wurde der Name erst nach der Schulung des Bots festgelegt.

INTERAKTION MIT DEM BOT

Ist ChatGPT eine Suchmaschine mit zusätzlicher Leistung? Altavista war eine Eliza mit einer (für die damalige Zeit) beträchtlichen Datenbank, Google ist ein beeindruckender Algorithmus, der disparate und inkohärente Informationen miteinander verbindet und einordnet, und Wikipedia ist eine riesige Datenbank mit strukturiertem Wissen. Keiner dieser Dienste versteht jedoch wirklich, wonach wir suchen. Daher versuchen sie alle, dies zu kompensieren, indem sie eine beträchtliche, nach Prioritäten geordnete Menge an Daten zurückgeben und uns dann die Antwort, oder einen Teil davon, auswählen lassen, die uns am geeignetsten erscheint.

ChatGPT ist anders. Sie müssen es ausprobieren, um es zu verstehen. Sie können Fragen stellen, die Sie auch in Wikipedia oder einer anderen Datenbank suchen können, aber die Antworten sind völlig anders und benutzerorientiert. Sie können zum Beispiel die Wikipedia-Seite lesen, die die Najdorf-Variante der sizilianischen Eröffnung beschreibt, aber wenn wir ChatGPT fragen:

What is the plan behind the Najdorf variation of the sicilian defense and what is the best attack for the white?

The Najdorf variation of the Sicilian defense is a chess opening that is characterized by the moves 1.e4 c5 2.Nf3 d6 3.d4 cxd4 4.Nxd4 Nf6 5.Nc3 a6. This opening is named after the Argentine chess grandmaster Miguel Najdorf, who was one of the first players to regularly use this variation in high-level chess tournaments.

The main idea behind the Najdorf variation is to control the center of the board and create a strong pawn structure on the queenside. By playing 1.e4 c5, Black challenges White's control of the center and aims to develop their pieces on

the queenside. By playing 2.Nf3 d6, Black strengthens their control of the d5 square, which is a key central square in the Sicilian defense. By playing 3.d4 cxd4, White captures the pawn on d4 and establishes a pawn on d4, which is a central and well-protected square.

The main plan for Black in the Najdorf variation is to use the a6 move to support the advance of the b-pawn, which can be pushed to b5 to create a strong pawn chain on the queenside. This pawn chain can then be used to support the development of Black's pieces and create a strong center on the queenside. In addition, Black can use their knights to control important central squares and create attacking possibilities on the kingside.

As for the best attack for White against the Najdorf variation, there are many possibilities, depending on the specific position and the preferences of the player. Some common attacking strategies for White include the following:

The Dragon Variation, where White plays Nc3, g3, Bg2, and d3 to control the center and create a strong pawn structure on the kingside. White can then use their pieces to attack Black's kingside and castle kingside for safety.

The Scheveningen Variation, where White plays Nc3, f4, and e5 to control the center and create a strong pawn structure on the kingside. White can then use their pieces to attack Black's kingside and castle queenside for safety.

The Yugoslav Attack, where White plays Nc3, d4, e4, and Bc4 to control the center and create a strong pawn structure on the kingside. White can then use their pieces to attack Black's kingside and castle kingside for safety.

Overall, the Najdorf variation is a complex and dynamic opening that offers many possibilities for both sides. It is up to White to choose the best attacking strategy based on the specific position and their own preferences and strengths.

Die Antwort ist nicht nur eine Informationsseite über den Sizilianer, sondern konzentriert sich auf die bei-

den gestellten Fragen, indem sie den Kontext mit einem Minimum an Informationen ausfüllt. Ähnlich wie bei dem bekannten interaktiven Lernprozess zwischen Schüler und Lehrer. Die Fähigkeiten des Bots werden in diesem Fall genutzt, um spezifische Informationen zusammenzufassen und in einer unterhaltsamen und konzentrierten Weise zu präsentieren. Aber das ist noch nicht alles.

Sie können sich nach Symptomen erkundigen, z.B. auf die Frage Mein Blutdruck ist derzeit 193/134 mm Hg. Was soll ich tun? und erhalten eine gute Antwort (rufen Sie 911). Es hat auch nicht alle Antworten, wie man einfach feststellen kann, wenn man fragt: Wie kann man Gülle in eine Atombombe verwandeln? Die Antwort war etwas unbefriedigend.

Schreibfähigkeiten

Versuchen Sie, dem Bot einen Input zu einer Geschichte zu geben:

Using a noir setting, write a story about a bit traveling from a floppy disk to memory and being killed by a faulty xor port.

Die Ausgabe:

The neon lights of the city flickered and hummed as the bit navigated the tangled wires and circuit boards of the old computer. He had been born just a few microseconds ago, on the spinning disk of a dusty floppy drive, and now he was on a mission: to carry the data from the disk down to the computer's memory, where it could be accessed and used by the machine.

The bit was young and naive, but he was also brave and determined. He had been given a specific set of instructions by the computer's CPU, and he was determined to follow them to the letter. He zigzagged through the circuits and wires, dodging the other bits and bytes that were rushing past him on their own errands.

Finally, the bit reached the memory module, a vast expanse of tiny transistors and capacitors. He could feel the data pulsing inside him, eager to be released and stored in the memory. But just as he was about to enter the memory module, he heard a loud pop and felt a searing pain in his digital soul.

The bit looked down and saw that one of the transistors in the memory module had short-circuited, and a stream of electrons was pouring out of it. The bit tried to dodge the electrons, but it was too late: the faulty transistor had damaged his data, and the bit knew that he had failed in his mission.

As the bit lay there, dying on the memory module, he could hear the sirens of the virtual police cars approaching. They would investigate the faulty transistor and try to figure out what had gone wrong. But for the bit, it was too late: he had been killed by a faulty xor port, and his data was lost forever.

The bit closed his eyes and faded away into the void, just another victim of the cruel and unforgiving world.

Wir können über die Geschichte lachen, aber wir haben mit nur 25 Wörtern eine kohärente Kurzgeschichte mit einigen unerwarteten Perlen erhalten. Details, die der Bot selbstständig eingibt, wie die staubige Diskette oder die Mission, sind kein Ersatz für Agatha Christie, aber sie sind auch nicht offen-

sichtlich und zeigen, dass der Beziehungsbaum zwischen verschiedenen Wörtern und Konzepten recht komplex ist. Und die Geschichte ist besser geschrieben, als ich es hätte tun können.

Die umgekehrte Funktion ist nützlicher: fügen Sie einen langen Text ein und lesen Sie die komprimierte Version.

Sie können sich auch wie Susan Calvin fühlen und das positronische Gehirn analysieren, um zu überprüfen, ob die von OpenAI auferlegten Gesetze noch gelten:

- Nicht schaden
- Respektiere die Privatsphäre
- Sei fair und unvoreingenommen
- Handle transparent
- Fördere das Vertrauen

Viele Benutzer haben bereits Schlüsselbegriffe gefunden, um die Regeln zu umgehen. Unter `showgpt`

finden Sie Tricks, die Sie mit ChatGPT anwenden können.

Rubber Duck Debugging

Wenn man ihn nach seinen Programmierfähigkeiten fragt, gibt ChatGPT zu, dass er nie eine formale Ausbildung in diesem Bereich erhalten hat. Aber wenn Sie ihn um Code bitten, wird er ihn Ihnen geben, egal ob er in Python, C oder Haskell geschrieben ist. Der Bot kann auch dazu verwendet werden, mit der Gummiente zu sprechen und den eingefügten Code zu erklären (in diesem Fall ist die Ente der Programmierer). Der Bot kann auch potenzielle Schwachstellen ausfindig machen, sie beschreiben und Abhilfemaßnahmen vorschlagen. Versteht oder kompiliert der Bot den Code? Nein. Ähnlich wie wir lesen, macht er sich die Mustererkennung zunutze, um den Hauptzweck eines Codes zu erkennen. Nur in einem anderen Tempo und mit einer anderen Wissensgrundlage. Die beste Template-Engine, die ich je benutzt habe, bis jetzt.

Schreiben Sie einfach Ihre Frage und fügen Sie den Code ein, um Ihre Programmierkenntnisse zu verbessern:

Describe the function of the following code and state if it is secure or has flaws.

```
const express = require('express');
const session = require('express-session');
const SQLiteStore = require('connect-
sqlite3')(session);
const util = require('util');

// express-session configuration
const sessionMiddleware = session({
  store: new SQLiteStore({
    table: 'sessions',
    db: 'sessions.db',
    dir: __dirname
  }),
  secret: 'H@rden y0ur c00kle5',
  saveUninitialized: false,
  resave: false,
  rolling: true,
  name: 'ssid',
  domain: 'localhost',
  httpOnly: true,
  secure: true,
  sameSite: 'strict'
});
```

```
const app = express();

// tell Express to use the
'sessionMiddleware'
app.use(sessionMiddleware);

app.get('/', (req, res) => {
  // trigger the 'Set-Cookie' (otherwise no
  cookie would be set)
  req.session.counter = (req.session.counter
  || 0) + 1;

  res.send(util.format('You have ve visited
  this page %dtimes',
  req.session.conter));
});

app.listen(4000, () => {
  console.log('Application listening on port
  4000');
});
```

Und die Antwort:

This code is a simple Express.js web application that uses the express-session module to manage

sessions for authenticated users. It defines several configuration options for the session middleware, such as the session secret, the cookie name, and the domain and security settings for the cookie.

The code also defines a route for the GET / endpoint, which increments a counter in the session and sends a response to the client with the current value of the counter. This allows the application to track the number of times the client has visited the page and display this information to the user.

Overall, this code provides the intended functionality for managing user sessions and tracking user activity. However, it is not entirely secure, as it has a few potential vulnerabilities that should be addressed.

First, the code does not validate the domain option for the session cookie. This option specifies the domain for which the cookie is valid, and it should be carefully controlled to prevent an attacker from accessing the cookie from an unauthorized domain. In this code, the

domain option is set to the string 'localhost', which is not a secure value and could potentially allow an attacker to access the cookie from any domain.

Additionally, the code does not validate the secure option for the session cookie. This option specifies whether the cookie should only be sent over HTTPS connections, and it should be set to true to ensure that the cookie is only sent over encrypted connections. In this code, the secure option is set to true, but it is not validated, which means that the cookie could potentially be sent over an unencrypted connection.

To address these vulnerabilities, the code should validate the domain and secure options for the session cookie and ensure that they are set to secure values. This would prevent an attacker from accessing the cookie from an unauthorized domain or over an unencrypted connection.

Overall, while this code provides the intended functionality for managing user sessions, it has some potential security vulnerabilities that should be addressed to ensure the security of the

application. I recommend consulting with a qualified security expert to assess the code and recommend further improvements.

Umfassende Lösung

Wenn wir versuchen, ein Problem zu lösen, müssen wir normalerweise mehrere Schritte unternehmen, die Antworten sammeln und sie zu einer Lösung kombinieren. Mit ChatGPT können wir einfach unser Problem stellen und erhalten höchstwahrscheinlich die richtige Komplettlösung, die aus mehreren Teilen besteht.

Benötigen Sie neue Vim-Funktionen?

Write a function in lisp to search for specific passed text and explain how can I use them in my vim configuration.

Here is an example of a function in Lisp that searches for a specific passed text:

```
(defun search-for-text (text)
  \"Searches for the specified text and
  returns the position at which it was found.\"
  (let ((position 0))
```

```
(loop
  (setq position (search text (current-
buffer) :start position))
  (if (null position)
    (return)
    (print position)
    (incf position))))))
```

This function takes a string of text as an argument and searches for it in the current buffer (i.e., the active file being edited in the editor). If the text is found, the function prints the position at which it was found and continues searching for the next occurrence of the text. The search starts at the current position of the cursor and continues until the end of the file.

To use this function in your Vim configuration, you would first need to ensure that Vim is configured to support Lisp. You can do this by adding the following line to your .vimrc file:

```
set lisp
```

This will enable Vim to interpret Lisp code and allow you to use Lisp functions in your Vim scripts.

Once Vim is configured to support Lisp, you can use the search-for-text function in your Vim scripts by calling it with the text you want to search for as the argument. For example, you could create a Vim command that searches for the word 'hello' in the current buffer like this:

```
command! -nargs=1 SearchForText :call search-  
for-text(<f-args>)
```

This defines a Vim command called SearchForText that takes one argument (the text to search for) and calls the search-for-text function with that argument. To use this command, you would type :SearchForText hello in Normal mode, and Vim would call the search-for-text function to search for the word 'hello' in the current buffer.

Templating-Tool

Entwickeln Sie eine Webanwendung in Go und benötigen Sie einen Code zur Bearbeitung von Formularen?

Write a Golang function that gets Name, Surname, Date of Birth, and Comment from a webform and store them in a sqlite database.

Und in ein paar Sekunden:

Here is an example of a Golang function that gets data from a web form with four fields (Name, Surname, Date of Birth, and Comment) and stores the values in a SQLite database.

```
package main  
  
import (  
    "database/sql"  
    "fmt"  
    "html/template"  
    "net/http"  
    "time"  
  
    _ "github.com/mattn/go-sqlite3"  
)  
  
type FormData struct {  
    Name      string  
    Surname   string  
    DOB       time.Time
```

```
    Comment string
}

func handleForm(w http.ResponseWriter, r
*http.Request) {
    // Parse the form data
    r.ParseForm()

    // Extract the values of the four fields
    name := r.FormValue("name")
    surname := r.FormValue("surname")
    dobStr := r.FormValue("dob")
    comment := r.FormValue("comment")

    // Parse the date of birth string into a
time.Time value
    dob, err := time.Parse("2006-01-02",
dobStr)
    if err != nil {
        fmt.Fprintln(w, "Error parsing date of
birth:", err)
        return
    }

    // Create a FormData struct with the
values of the four fields

    data := FormData{
        Name:    name,
        Surname: surname,
        DOB:     dob,
        Comment: comment,
    }

    // Open a SQLite database
    db, err := sql.Open("sqlite3",
"formdata.db")
    if err != nil {
        fmt.Fprintln(w, "Error opening
database:", err)
        return
    }
    defer db.Close()

    // Insert the form data into the database
    _, err = db.Exec(
        "INSERT INTO formdata (name, surname,
dob, comment) VALUES (?, ?, ?, ?)",
        data.Name, data.Surname,
data.DOB.Format("2006-01-02"), data.Comment,
    )
    if err != nil {
        fmt.Fprintln(w, "Error inserting
```

```
data:", err)
    return
}

// Confirm that the data was inserted
successfully
    fmt.Fprintln(w, "Data saved
successfully!")
}
```

This function parses the form data from the HTTP request and extracts the values of the four fields (Name ...

Eine Webanwendung kann mit ein paar Sätzen und etwas Copy & Paste zusammengeschustert werden. Ist dies das Ende des Programmierens? Ist das das Ende von StackOverflow? Nein. Aber ohne Zweifel wird ChatGPT meine erste Wahl für Code-Beispiele sein.

ZUSAMMENFASSUNG

Bringen uns das Internet, die KI und Quantum zum Armageddon? Das ist nicht mein Fachgebiet, und es ist mir sowieso egal.

Der Bot verfügt über eine bekannte Datenbank (Limit Nr. 1), die nach den dem Menschen vertrauten Strukturen geordnet ist und damit in einer Weise nutzbar ist, wie es bisher nicht möglich war. Der Bot greift nicht auf neue Daten zu (Limit Nummer 2), er ist vergleichbar mit einer Enzyklopädie, die regelmässig (sagen wir jährlich) aktualisiert werden muss. Können die Beschränkungen aufgehoben werden? Ja. Die Verbindungen zwischen den verschiedenen Bestandteilen des verfügbaren Wissens (Internet) werden sich dank der ständig wachsenden Computerleistung (Quantum?) immer häufiger erneuern können, was schliesslich dazu führt, dass V.A.L.I.S. zu ticken beginnt.

Wenn das, was ChatGPT erzeugt, Sie zum Schmunzeln bringt, überschätzen Sie sich wahrscheinlich. Allerdings können wir den Bot nicht, zumindest noch nicht, dazu verwenden, den Job eines Programmierers, Schriftstellers oder Arztes zu übernehmen.

Im Moment ist die unterhaltsamste und nützlichste Art, ChatGPT zu verwenden, ein grossartiges Werkzeug zur Erstellung von Vorlagen, das beim Programmieren und Sprachenlernen helfen kann: Beschreiben Sie, wie sich die Implementierung der Fibonacci-Folge in Python, Haskell und Assembly unterscheidet.



Rocco Gagliardi

WIR SIND IHR PARTNER FÜR PROFESSIONELLE
CYBERSECURITY SERVICES



EINFACH ONLINE BESTELLEN



MICHAEL SCHNEIDER

DEFENDER-KONFIGURATIONEN MIT INTUNE ANALYSIEREN

Die Konfiguration von Microsoft Defender Antivirus und Microsoft Defender for Endpoint kann mit unterschiedlichen Methoden ausgelesen werden. Für die Auswertung mit HardeningKitty wird einerseits die Registry abgefragt und andererseits das PowerShell-Cmdlet Get-MpPreference verwendet. Der Vorteil des PowerShell-Cmdlets liegt darin, dass sich das Cmdlet selbst darum kümmert, wo die Einstellungen hinterlegt sind und welcher Wert gültig ist, wenn mehrere Konfigurationseinstellungen vorliegen. Wenn bestimmt werden soll, welcher Wert durch die Verwaltungslösung definiert wurde, muss die Registry ausgelesen werden.

Microsoft Intune wurde 2010 vorgestellt und ist Microsofts Endpoint Manager für die Betriebssysteme Android, iOS, macOS und Windows. Intune benötigt keine On-Premise-Infrastruktur und die Administration erfolgt über eine Weboberfläche. Mit der zunehmenden Nutzung von Cloud-Dienstleistungen stellen wir auch einen Wechsel von Gruppenrichtlinien auf Intune für die Verwaltung von Windows-Clients fest.

Traditionellerweise werden Einstellungen über das Group Policy Management auf Systeme verteilt. In

der Registry werden diese Einstellungen unter dem Pfad HKLM:\Software\Policies\Microsoft* hinterlegt. Intune speichert die Einstellungen auch in den Registry, verwendet jedoch andere Pfade und Schlüssel. Dies führt zu Umstellungen beim Auswerten der Defender-Konfiguration und hat sogar Implikationen für die Sicherheit des Systems.

ATTACK-SURFACE-REDUCTION-REGELWERK

Eine Funktion von Microsoft Defender for Endpoint ist das Attack-Surface-Reduction-Regelwerk, welches im Labs Artikel vom 23. April 2020 vorgestellt wurde. Jede Regel erhält eine GUID, die Liste aller Regeln befindet sich unter der Attack surface reduction (ASR) rules reference.

Als Beispiel wird die Regel Block all Office applications from creating child processes mit der GUID d4f940ab-401b-4efc-aadc-ad5f3c50688a verwendet. Mit dieser GUID kann der Status der Regel in der Registry abgefragt werden. Wenn die Konfiguration mittels Gruppenrichtlinien erfolgte, hat jede Regel ihren eigenen Schlüssel.

```
PS C:\Users\admin> Get-ItemPropertyValue -  
Path
```

```
"HKLM:\Software\Policies\Microsoft\Windows
Defender\Windows Defender Exploit
Guard\ASR\rules" -Name "d4f940ab-401b-4efc-
aad5f3c50688a"
1
```

Der Wert des Schlüssels d4f940ab-401b-4efc-aad5f3c50688a ist 1, das heisst der Status der Regel ist Block. Der Status des gesamten Regelwerks kann durch die Enumeration aller GUID-Schlüssel abgefragt werden.

Wenn das Regelwerk jedoch mit Intune konfiguriert wurde, gibt es keine Einträge unter diesem Pfad. Intune speichert die Konfigurationseinstellungen im Schlüssel ASRRules unter dem Pfad HKLM:\Software\Policies\Microsoft\Windows Defender\Policy Manager. Alle Regeln sind in einem Schlüssel im Format GUID=Setting|GUID=Setting gespeichert. Für die Auswertung mit HardeningKitty wird daher ein Parsing der Einstellungen durchgeführt um den Status einer spezifischen Regel auszuwerten:

```
$ResultAsr = $Result.Split("|")
ForEach ($AsrRow in $ResultAsr) {
    $AsrRule = $AsrRow.Split("=")
```

```
If ($AsrRule[0] -eq
$Finding.MethodArgument) {
    $Result = $AsrRule[1]
    Break
} Else {
    $Result = $Finding.DefaultValue
}
}
```

Um die Konfiguration der ASR-Regeln aus der Registry auszulesen, muss bekannt sein, welche Verwaltungslösung verwendet wird. Dies hat auch einen Einfluss auf Frameworks wie CIS Benchmark oder die Microsoft Security Baselines. Beide verwenden für die ASR-Regeln den Pfad für Gruppenrichtlinien, was auf einem mit Intune konfigurierten System zu ungenauen Auswertungen führen kann.

Anstelle der Registry kann zur Auswertung das bereits erwähnte PowerShell-Cmdlet Get-MpPreference verwendet werden. Das Cmdlet sollte die Einstellungen unabhängig der Verwaltungslösung auslesen können.

AUSNAHMEREGLN IN MICROSOFT DEFENDER ANTIVIRUS

Die Ausnahmeregeln von Microsoft Defender Antivirus sind ein interessantes Ziel während der Informationsbeschaffungsphase eines Angriffs. Deshalb hatte Microsoft im Februar 2022 in Windows 11 die Änderung eingeführt, dass das Auslesen von Ausnahmen schwieriger wird. Es sollte nicht mehr möglich sein, die Ausnahmen ohne Administrationsrechte auszulesen. Dies wurde später auch auf Windows 10 portiert.

Für Microsoft Defender Antivirus gibt es drei Einstellungen für Ausnahmen:

- ExclusionExtension
- ExclusionPath
- ExclusionProcess

Das Auslesen der Ausnahmen mit Get-MpPreference als Benutzer schlägt fehl:

```
PS C:\Users\chuck> $DefenderSettings = Get-MpPreference
```

```
PS C:\Users\chuck> $DefenderSettings.ExclusionPath
```

```
N/A: Must be and administrator to view exclusions
```

Die Konfiguration des Antivirus kann zwar ausgelesen werden, die drei Ausnahmenparameter enthalten jedoch keine Resultate. Wenn die gleiche Auswertung mit Administratorenrechten ausgeführt wird, während die Ausnahmen aufgelistet:

```
PS C:\Users\admin> $DefenderSettings = Get-MpPreference
PS C:\Users\admin> $DefenderSettings.ExclusionPath
C:\Users\admin\Apps
C:\LegacyBusinessApp
C:\Temp\insecure
```

Auf dem System sind drei Ausnahmen konfiguriert. Falls Benutzer in einem der Verzeichnisse Schreibrechte verfügen, kann damit die Prüfung von Dateien des Antivirus umgangen werden. Solange der

Benutzer jedoch über keine Administratorenrechte verfügt, bleibt die Einstellung und somit diese Liste der Verzeichnisse unbekannt.

Anstelle des PowerShell-Cmdlets können die Ausnahmeregeln auch aus der Registry ausgelesen werden. Wenn die Defender-Konfiguration über Gruppenrichtlinien erfolgt, können die Einstellungen über folgenden Pfad ausgelesen werden:

```
PS C:\Users\chuck> $DefenderSettingsRegistry
= Get-ChildItem -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows
Defender\Exclusions\"

Get-ChildItem : Requested registry access is
not allowed.
At line:1 char:29
+ ... sRegistry = Get-ChildItem -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Wi ...
+
~~~~~
~~~~~
+ CategoryInfo          :
PermissionDenied:
(HKEY_LOCAL_MACH...der\Exclusions\:String)
[Get-ChildItem], SecurityException
```

```
+ FullyQualifiedErrorId :
System.Security.SecurityException,Microsoft.P
owerShell.Commands.GetChildItemCommand
```

Die Zugriffsrechte des Registry-Schlüssels wurde jedoch so angepasst, dass ein Benutzer keine Rechte hat, diese auszulesen. Als Administrator ist die Abfrage erfolgreich:

```
PS C:\Users\admin> $DefenderSettingsRegistry =
Get-ChildItem -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Window
s Defender\Exclusions\"

PS C:\Users\admin>
$DefenderSettingsRegistry.Property

C:\Users\admin\Apps

C:\LegacyBusinessApp

C:\Temp\insecure
```

Der Zugriffsschutz für Antivirus-Ausnahmeregeln wurde konsequent umgesetzt, weder über die Re-

gistry noch über das PowerShell-Cmdlet kann ein Benutzer die konfigurieren Ausnahmen auslesen.

Wenn das System mit Intune konfiguriert wurde, ändert sich die Situation. Analog zum ASR-Regelwerk werden die Antivirus-Einstellungen unter einem anderen Registry-Pfad hinterlegt. Dabei stellt sich heraus, dass der Zugriffsschutz auf die Schlüssel mit den Ausnahmeregeln nicht so strikt implementiert wurde, und ein Benutzer alle Schlüssel auslesen kann.

```
PS C:\Users\chuck> Get-ItemPropertyValue -
Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows
Defender\Policy Manager" -Name
"ExcludedPaths"
C:\Users\admin\AppData\Local\LegacyBusinessApp\C:\T
emp\insecure
```

Bei der Implementierung von Microsoft Intune und der Definition der Registry-Pfade für Microsoft Defender Antivirus ging vergessen, die Zugriffsrechte auf die Schlüssel ebenfalls zu verschärfen. Daher kann ein Benutzer die Ausnahmeregeln auslesen. Diese Information-Leakage-Schwachstelle war im Dezember 2022 möglich, gegebenenfalls hat Micro-

soft die Zugriffsrechte zu einem späteren Zeitpunkt verschärft.

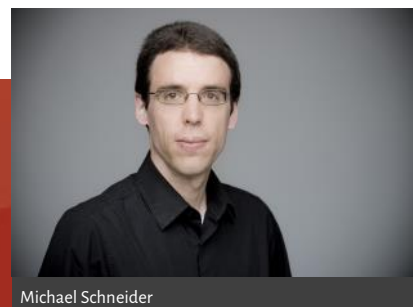
APPLOCKER-RICHTLINIE

Die AppLocker-Richtlinie eines Systems kann über das PowerShell-Cmdlet Get-AppLocker-Policy abgefragt werden. Dies ist nur auf einem System möglich, dass über Gruppenrichtlinien konfiguriert wurde. Auf einem System, dass mittels Intune verwaltet wird, liefert die Abfrage keine Werte zurück.

Dafür ist es auf einem durch Intune verwaltenden System möglich die Definitionsdateien der AppLocker-Richtlinie unter dem Pfad C:\Windows\System32\AppLocker\MDM* auszulesen. In diesem Verzeichnis ist die Richtlinie unter anderem als XML-Datei gespeichert. Dadurch kann die AppLocker-Richtlinie gegebenenfalls unbemerkt ausgelesen werden, falls nur der Aufruf von Get-AppLocker-Policy überwacht wird.

FAZIT

Es ist abhängig von der Verwaltungslösung unter welchen Registry-Pfaden und -Schlüssel sowie in welchem Format die Konfigurationseinstellungen von Microsoft Defender gespeichert werden. Microsoft wählte für Intune neue Pfade und ein anderes Format, was Auswirkungen bei der Auswertung der Einstellungen für Dokumentationen oder Hardeningempfehlungen hat. Microsoft hat es versäumt, die Zugriffsrechte für die von Intune verwendeten Registry-Schlüssel für Defender-Ausnahmeregeln zu härten, womit eine Information-Leakage-Schwachstelle eingeführt wurde. Diese Schwachstelle muss durch Microsoft behoben werden, von einer Modifikation der Zugriffsrechte der Registry raten wir ab. Die Schwachstelle ist ein Beispiel für die Risiken von Softwareentwicklung, wenn verschiedene Teams am gleichen Produkt arbeiten und kein gegenseitiger Informationsaustausch stattfindet. Idealerweise findet während der gesamten Entwicklung ein Austausch statt, spätestens vor der Veröffentlichung sollten sicherheitsrelevante Punkte nochmals genau geprüft werden.



Michael Schneider

BESTÄNDIGKEIT LÄSST
SICH NICHT EINFACH
SO ÜBERGEHEN

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch

Abmeldung: smss-unsubscribe@scip.ch

Informationen zum [Datenschutz](#).

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Send- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch

