

Ransomware, Spyware, Malware, Virus – so schützen Sie Ihre IBM i

Auch die IBM i ist gegen Bedrohungen nicht immun. Schützen und sichern Sie Ihre geschäftskritischen Daten, erkennen Sie Schwachstellen und nutzen Sie Echtzeitwarnungen.

We Know How.



AGENDA

01

Wie sicher ist Ihre IBM i?

02

Wie sieht eine Verteidigungsstrategie auf der IBM I aus?

03

Wie können Sie ein Security System auf der IBM I einsetzen?



**SYSTEM
HACKED**

```
var ts = d.createElement("script");  
ts.type = "text/javascript";  
ts.async = true;  
ts.id = id;  
ts.src = "https://www.example.com/";  
var f = function () {  
  var s = d.getElementsByTagName("script");  
  s.parentNode.insertBefore(ts, s);  
};  
if (%opr == "object") {  
  d.addEventListener("load", f);  
}
```

```
<div class="warning">  
  <div class="triangle">  
    <div class="exclamation">  
      </div>  
    </div>  
  </div>  
</div>  
</form>  
</div>  
</script>  
function openForm() {  
  let form = document.getElementById("form");  
  form.classList.remove("hidden");  
  form.setAttribute("aria-hidden", "false");  
  form.querySelector("#input").focus();  
}
```

```
document, window, "topall-";  
</script>  
<script type="text/javascript">  
  var bar = document.getElementById("bar");  
  bar.push(1);  
  bar.id = "page1";  
  bar.type = "page1";  
</script>  
<script type="text/javascript">  
  (function(d, s) {  
    var js = d.createElement(s);  
    js.type = "text/javascript";  
    js.async = true;  
    js.src = "https://www.example.com/";  
    var f = function () {  
      var s = d.getElementsByTagName("script");  
      s.parentNode.insertBefore(js, s);  
    };  
    if (%opr == "object") {  
      d.addEventListener("load", f);  
    }  
  })(document, "script");  
</script>
```

```
var ts = d.createElement("script");  
ts.type = "text/javascript";  
ts.async = true;  
ts.id = id;  
ts.src = "https://www.example.com/";  
var f = function () {  
  var s = d.getElementsByTagName("script");  
  s.parentNode.insertBefore(ts, s);  
};  
if (%opr == "object") {  
  d.addEventListener("load", f);  
}
```

```
var ts = d.createElement("script");  
ts.type = "text/javascript";  
ts.async = true;  
ts.id = id;  
ts.src = "https://www.example.com/";  
var f = function () {  
  var s = d.getElementsByTagName("script");  
  s.parentNode.insertBefore(ts, s);  
};  
if (%opr == "object") {  
  d.addEventListener("load", f);  
}
```

Wie sicher ist Ihre IBM i?

Kennen Sie Dimitri Badin?

ER IST „DER MANN IN MERKELS RECHNER“

Nach Hackerangriff auf Bundestag

EU verhängt Sanktionen gegen russische Geheimdienstler

Von afp 22.10.2020
Lesedauer: 1 Min.



Dimitri Badin auf einem Fahndungsplakat des FBI: Laut Medienberichten wird ihm der Hackerangriff auf den Bundestag vorgeworfen. (Quelle: FBI/Getty Images/t-online.de)

„t-online.de; afp; „EU verhängt Sanktionen gegen russische Geheimdienstler“;
22.10.2020

Wussten Sie, dass...

...**67%** DER UNTERNEHMEN IN DEUTSCHLAND 2021 OPFER VON RANSOMWARE ANGRIFFEN WAREN?¹

...**42%** DER UNTERNEHMEN ANGABEN, DASS SIE BEREITS MINDESTENS EINEN ANGRIFF ERLEBT HABEN.²

...**24%** DER ANGRIFFE FÜR ZWEI MONATE ODER SOGAR LÄNGER UNENTDECKT BLIEBEN.²

... CA. **146.000** CYBERANGRIFFE IN DEUTSCHLAND 2021 POLIZEILICH GEMELDET WURDEN.¹

... DER GESAMTSCHADEN DURCH CYBERCRIME SICH IN 2021 AUF **€ 223,5 MRD.** ALLEINE IN DEUTSCHLAND BELIEF.¹ **DAS SIND 6% DES BIP ODER MEHR ALS DER „DOPPELWUMMS“**

... DIE DURCHSCHNITTLICHE LÖSEGELDSUMME BEI RANSOMWAREANGRIFFEN IN 2021 BEI **€ 250.000** LAG.¹

¹ Quelle: BKA, Bundeslagebild Cybercrime 2021; Ausgabe 2022, 09. Mai 2022

² Quelle: Fresche, IBM & Forbes/cybersecurity-in-2022c

Und wussten Sie, dass...

...**45%** DER UNTERNEHMEN IN DEUTSCHLAND DER AUSSAGE ZUSTIMMEN, DASS „CYBERANGRIFFE IHRE GESCHÄFTLICHE EXISTENZ BEDROHEN“ (GEGENÜBER 9% IN 2021!)¹

...**78%** DER UNTERNEHMEN DAVON AUSGEHEN, DASS DIE ZAHL DER ANGRIFFE IN DEN NÄCHSTEN 12 MONATEN ZUNEHMEN WIRD.¹

TROTZ DIESER SELBSTEINSCHÄTZUNG DER UNTERNEHMEN WIRD BISHER RELATIV WENIG FÜR IT-SICHERHEIT AUSGEGEBEN (2022 CA. 9% DES GESAMTEN IT-BUDGETS, 2021 7%).

¹ Quelle: Bitkom research 2022; 31. August 2022

Was bedeutet das für IBM i Systeme?

- DIE IBM I IST EINE SICHERE PLATTFORM - WENN SIE RICHTIG KONFIGURIERT UND PERMANENT ÜBERWACHT WIRD.
- ABER AUCH DIE IBM I IST GEGEN BEDROHUNGEN NICHT IMMUN. GENERELL IST JEDES SYSTEM POTENZIELL GEFÄHRDET – AUCH IBM I KUNDEN WERDEN REGELMÄßIG OPFER VON ANGRIFFEN.
- JEDER CYBERANGRIFF IN IHREN NETZWERKEN, EGAL WELCHES „EINFALLSTOR“ BENUTZT WIRD, STELLT AUCH IMMER EINEN ANGRIFF AUF IHR IBM I SYSTEM DAR.



Wie sieht eine Verteidigungsstrategie auf der IBM i aus?

Unsere IBM i - Verteidigungsstrategie

Auditing & Compliance

IBM i Security Prüfung und Kontrolle mit integriertem Berichtswesen zur Einhaltung der IBM i Security-Richtlinien.

Schutz vor Malware

Tracking und Zugriffssperre auf Protokollebene und Sicherung des integrierten Filesystems (IFS).

Angriffserkennung mit SIEM* Integration

Echtzeitüberwachung und Alarm bei Sicherheitsvorfällen

Datenverkehr Absicherung

Überwachung des IBM i Datenverkehr

Datenverschlüsselung

Verschlüsselung, Maskierung und Anonymisierung von zu schützenden Daten

* *Security Information & Event Management*

Unsere IBM i Verteidigungsstrategie mit der Trinity Guard Suite 3.0



Trinity Guard – „Green Screen“ & Management Konsole

TGMENUD TG - Main Menu

System: SPGTEST

Select one of the following:

1. TGAudit
2. TGSecure
3. TGDetect
4. TGEncrypt

10. TGCentral Configuration

20. Save/Restore Configuration

70. Work with TG Product Users

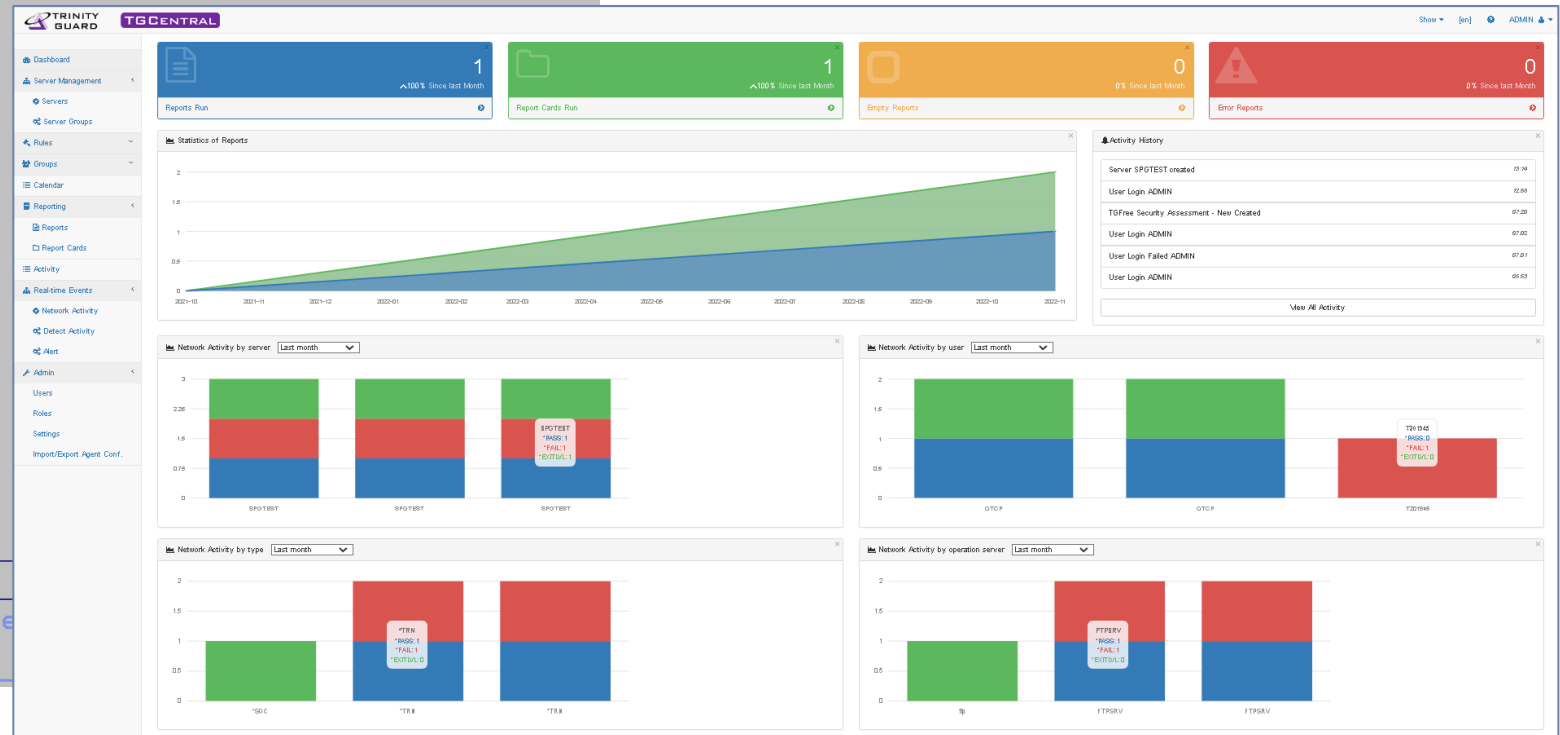
80. Licensing Status

Selection or command

==> █

F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Copyright © 2013-2022 Trinity Guard LLC. All



TG SECURE – Zugriff Sicherheit

TG SECURE

- Schutz der IBM i Server vor externen und internen Sicherheitsbedrohungen
- Überwachung des gesamten Netzwerkverkehrs
- Warnung vor kritischen Netzwerkbedrohungen
- Möglichkeit, das Netzwerk vor internen und externen Angriffen zu schützen
- Schutz vor Malware (Schadprogramme wie z.B. Ransomware, Trojaner, Virus etc.)

TG AUDIT – Compliance & Auditing

TG AUDIT

- Compliance und Betrugsaufdeckung bzw. /-prävention
- Interne Audits sowie aufsichtsrechtliche, regulatorische Anforderungen für externe Audits
- Aufdecken von Änderungen in der Datenbank, die ihre Integrität gefährden können (z.B. direkte Änderungen durch DFU (Database File Utility) oder Änderungen direkt in der Datenbank ohne Kontrolle
- Einhaltung und Überwachung zahlreicher Regularien wie HIPAA, PCI-DSS, SOX und mehr
- Integrierte Berichtsvorlagen für die wichtigsten Compliance-Vorschriften
- Überwachung der Aktivitäten der berechtigten Nutzerkonten

TG ENCRYPT – Datenverschlüsselung

TG ENCRYPT

- Schutz sensibler Daten vor unbefugtem Zugriff durch
 - Verschlüsselung
 - Maskierung
 - Anonymisierung
- Überwachung des Zugangs zu sensiblen Daten auf Feldebene
- Warnung bei Änderungen auf Feldebene

TG DETECT – Echtzeitüberwachung & SIEM Integration

TG DETECT

- Echtzeit-Überwachung aller kritischen IBM i-Ereignisse
- Überwachung von Message Queues und Verlaufsprotokollen
- Echtzeit-Journal-Überwachung
- Ausführungsüberwachung bei kritischen Befehlen
- SIEMS Integration zur Konsolidierung von Sicherheits- und Betriebsereignissen
- Integration mit verschiedenen SIEMS auf dem Markt
(QRadar, Splunk, Graylog ArcSight, LogRhythm, AlienVault, MacAfee, usw.)

Wir bieten Ihnen konkret...

...IHREN SICHERHEITSTATUS AUF EINEN BLICK:

- MIT DEM SECURITY-ASSESSMENT WERDEN POTENZIELLE SCHWACHSTELLEN AUF IHRER IBM I AUFGEDECKT.
- DIE ERGEBNISSE WERDEN DETAILLIERT IN EINEM BERICHTS-PROTOKOLL AUFGEZEIGT, SO DASS SIE EINEN LEICHT VERSTÄNDLICHEN ÜBERBLICK ÜBER DEN ALLGEMEINEN SICHERHEITSTATUS IHRER IBM I ERHALTEN.
- DARÜBERHINAUS ERHALTEN SIE DETAILLIERTE EINZELBERICHTE, DIE IHNEN JEDE EINZELNE SCHWACHSTELLEN EXPLIZIT ERLÄUTERT.





VEREINBAREN SIE EINEN TERMIN MIT UNS.

WIR ZEIGEN IHNEN, WIE SIE
TRINITY GUARD IN IHREM UNTERNEHMEN
EINSETZEN KÖNNEN.

Kai Wiens

Sales Director

Specific-Group Germany GmbH

Kai.wiens@specific-group.com

M: +49 (0) 171 818 7976

Božidar Ivezić

Senior Developer & Technical Sales

Specific-Group Germany GmbH

Bozidar.ivecic@specific-group.com

M: +49 (0) 162 15 88 003

SICHERN SIE IHRE IBM I SYSTEME!



Alles, was Sie über uns und die IBM i wissen müssen!



www.as400entwicklung.com