

Mit freundlicher Unterstützung vom:



## Agenda der BGNW Frühjahrstagung am 23. und 24. März 2023 in München-Garching

### Sichere IT Aufbau und Betrieb robuster Systeme

#### Mittwoch, 22.03.2023

|             |  |
|-------------|--|
| ab<br>19:30 | Treffen für alle Tagungsteilnehmer, die bereits angereist sind, im <b>Gasthof zur Mühle</b> , Kirchplatz 5, 85737 Ismaning, Tel. 089-960930, Web: <a href="http://www.hotel-muehle.de">www.hotel-muehle.de</a> |
|-------------|--|

#### Donnerstag, 23.03.2023

Moderation: Hansjörg Ast, Thilo Hospe

|       |   |
|-------|---|
| 8:50  | Registrierung und Begrüßung   |
| 9:15  | <b>Erfahrungsbericht: Physische Sicherheit im Rechenzentrum</b><br>Planung von Einbruchmeldeanlagen, Videoüberwachung und organisatorischen Maßnahmen zur Zutrittskontrolle – ein Balanceakt konfliktierender Zielsetzungen.<br>Miran Mizani, Leibniz-Rechenzentrum   |
| 9:45  | Diskussion / Pause  |
| 10:05 | <b>Elemente einer sicheren &amp; robusten Netzwerkarchitektur</b><br>Funktionen zur Erleichterung von Betrieb und Wartung sowie die Absicherung der Infrastrukturkomponenten gegen Angriffe. Fokus: Datenübertragung außerhalb des gesicherten Perimeters (Campus) z.B. über Dark Fiber / öffentlichen Grund; Einsatz von IEEE 802.1AE MACsec.<br>Benjamin Eggerstedt, Alcatel-Lucent Enterprise  |
| 10:50 | Diskussion / Pause  |
| 11:10 | <b>Der Endpoint im Wandel. Moderne Sicherheit. Lösungsansätze u. a. mit ZTNA und SASE.</b><br>Neuer Ansatz zur Absicherung von Applikationen. Homogene Autorisierung von internen und externen Remote Usern und Büromitarbeitern (und allgemein Netzwerkendsystemen) in einem System.<br>Kurt Semba, Extreme Networks   |
| 11:55 | Diskussion  |
| 12:05 | <b>Mittagspause</b>   |
| 13:05 | <b>Privilegierte Konten und deren Zugriffe absichern!</b><br>Unberechtigte Zugriffe auf Systeme mit privilegierten Konten stellen ein erhöhtes Risiko dar. Eine einheitliche Lösung für die Absicherung von Remotezugriffen und die Erfüllung rechtlicher Vorgaben im Unternehmen ist geboten. Gezeigt wird, wie dies, trotz der Komplexität, an einem Tag mit einem großen Mehrwert implementiert werden kann.<br>Manfred Warta, Zeljko Stankovic – Fudo Security DACH |
| 13:50 | Diskussion / Pause  |
| 14:10 | <b>Erfahrungsbericht: Firewalls übersichtlich konfigurieren mittels Templates</b><br>Wie an der Universität Ulm das Problem unübersichtlicher Firewall-Konfigurationen mit Hilfe von Templates praxisorientiert gelöst wird.<br>Karl Gaissmaier, Universität Ulm  |
| 14:40 | Diskussion / Pause  |
| 15:00 | <b>Mitgliederversammlung der BGNW</b>   |
| 16:00 | Ende des ersten Tages   |

|             |   |
|-------------|---|
| 16:30       | Besichtigung des Großrechners im Leibniz-Rechenzentrums (ca. 1,5 Std.)  |
| ab<br>19:00 | Treffen für alle Tagungsteilnehmer im <b>Garching Augustiner</b> , Freisinger Landstraße 4, 85748 Garching, Tel. 089-20966739, Web: <a href="http://www.garching-augustiner.com">http://www.garching-augustiner.com</a> |

## Agenda der BGNW Frühjahrstagung am 23. und 24. März 2023 in München-Garching

### Sichere IT Aufbau und Betrieb robuster Systeme

#### Freitag, 24.03.2023

Moderation: Hansjörg Ast, Thilo Hospe

|       |   |
|-------|---|
| 8:15  | Registrierung und Begrüßung   |
| 8:30  | <b>Erfahrungsbericht: Aufbau des 5G-Campusnetzes an der TH Lübeck</b><br>An der TH Lübeck wurde ein 5G-Campusnetz auf Basis von Open Source Software sowie kommerziellen Produkten aufgebaut. Im Beitrag werden die gesammelten Erfahrungen sowie die Leistungsfähigkeit und Sicherheit des Netzes dargestellt.<br>Andreas Hanemann, TH Lübeck  |
| 9:15  | Diskussion / Pause  |
| 9:30  | <b>Cyber Risiken aus der Hackerperspektive</b><br>Tim Philipp Schäfers, OEDIV   |
| 10:15 | Diskussion / Pause  |
| 10:30 | <b>DNS – DAS unbeachtete Einfallstor für eine Vielzahl von Attacken</b><br>In 13 der Top 15 Angriffsszenarien spielt DNS eine gewichtige Rolle. Ob Malware, Ransomware, Phishing, Cryptojacking oder ähnliches, DNS wird immer häufiger für unterschiedliche Zwecke missbraucht. Der Sicherheitsaspekt wird beim Protokoll DNS häufig unzureichend berücksichtigt. Gezeigt wird, wie man Gefahren erkennt und DNS optimal nutzt für eine ganzheitliche Sicherheit des Unternehmens.<br>Benjamin Polak und Sebastian Hein, Infoblox  |
| 11:00 | Diskussion / Pause  |
| 11:15 | <b>Angriffe auf IT-Systeme - Live Hacking Demonstration</b><br>Sensibilisierung für Angriffs-Risiken in komplexen Systemen.<br>Sebastian Schreiber, SySS GmbH   |
| 11:45 | Diskussion  |
| 12:00 | <b>Mittagspause</b>   |
| 12:45 | <b>Erfolgreiche Umsetzung von Netzwerk Zugangskontrolle von einfach bis hochsicher</b><br>Zugangskontrolle, um die kritische Ressource Netzwerk abzusichern, sollte heute selbstverständlich sein. Entgegen stehen aber oft Bedenken, dass es zu Zugriffsproblemen kommen könnte oder der Administrationsaufwand zu hoch wird. Wir besprechen Wege zu einer erfolgreichen automatisierten Umsetzung, die alle Use Cases berücksichtigen und je nach Bedarf verschieden starke Sicherheit etablieren. Alles zentral und einfach zu verwalten.<br>Reinhard Lichte, Hewlett Packard Enterprise / Aruba |
| 13:30 | Diskussion / Pause  |
| 13:45 | <b>KI-gestützter Betrieb und Management von komplexen IT-Infrastrukturen und Rechenzentren (mit Erfahrungsbericht)</b><br>Die zunehmende Komplexität und Anzahl von Assets und Hosts im IT-Umfeld erfordert Innovation, Sicherheit und ressourcen-effizientes Management dieser Strukturen. Passive Netze werden mit aktivem Netzwerk-Equipment dokumentiert und live gemonitort. Mit Hilfe von künstlicher Intelligenz wird das Rechenzentrum vor Ausfällen geschützt und die Energieeffizienz gesteigert.<br>Jan Moll, dtm Datentechnik Moll GmbH   |
| 14:15 | Diskussion / Pause  |
| 14:30 | <b>Diskussion mit den anwesenden Referenten und Resumee der Tagung</b>  |
| 15:00 | Ende der Tagung   |