Cyber Digital

5. Cyberkongress

Ursprung der Hackerangriffe bis vor dem Krieg....

Ein kaum wahrnehmbarer, aber nicht unwichtiger Teil des Kriegs gegen die Ukraine spielt sich im Cyberspace ab. Microsoft hat in den vergangenen vier Monaten vermehrt russische Hackerangriffe festgestellt.

Experten von Microsoft haben seit Beginn des russischen Angriffskriegs gegen die Ukraine in 42 Ländern Attacken russischer Hacker festgestellt. Insgesamt seien 128 Organisationen betroffen, teilte das Unternehmen mit.

5. Cyberkongress

Aktuell ist es “ruhig”

Im Moment ist die Situation am Cybermarkt “ruhig”, die Versicherer verzeichnen einen starken Rückgang der erfolgreichen Angriffe.

60%

60%

Einige Versicherer haben bis zu 60% weniger Cyberschäden als noch vor einem Jahr.

5. Cyberkongress

Ruhe vor dem Sturm…

Experten sind sich einig, dass wir aktuell die “Ruhe vor dem Sturm” haben…

01. **Internet**

In Russland wurde die Bandbreite verringert, dadurch laufen Angriffe nicht so wie gewünscht.

02. **Verteidigung**

Russland wird massiv angegriffen und setzt die Cracker zur Verteidigung der Unternehmen ein.

5. Cybercongress

Conti-Hackergruppe

Die Ransomware-Bande «Conti» zeichnet für einige der **verheerendsten Hackerangriffe** der jüngeren Geschichte verantwortlich.

Conti gilt als eine der weltgrössten und gefährlichsten Ransomware-Banden – mit Dutzenden aktiven Mitgliedern mutmasslich in Russland und anderen osteuropäischen Ländern.

Die Conti-Ransomware tauchte erstmals im Mai 2020 auf. Was das Schadprogramm von anderen Malware-Stämmen unterscheidet, ist laut IT-Sicherheitsexperten die Geschwindigkeit, mit der es sich in fremden Netzwerken auf verschiedene Systeme ausbreiten kann und die Dateien verschlüsselt. Betroffen sind nicht nur Windows- sondern auch Linux-Systeme.

5. Cyberkongress

Conti - Auflösung

Die Hackergruppe hat sich im Juni 2022 aufgelöst.

Aufgrund des Ukranine-Krieges und der damit verbundenen Verwerfungen innerhalb der Gruppe wurde die Auflösung bekannt gegeben.

Ist dies eine gute Entwicklung für die IT-Sicherheit auf der Welt?

Nein…

Die Gruppe teilt sich auf und bringt das Know-How auch in andere Gruppen rein.

Zusammenarbeit

Die Führungsebene der Gruppe will auch weiterhin zusammenarbeiten.

5. Cybercongress

Sixt gehackt

Daten wurden erbeutet

Nach einem Cyberangriff auf die Autovermietung *Sixt* hat das Unternehmen zunächst angegeben, dass keine Daten entwendet worden seien. Nun musste diese Einschätzung korrigiert werden.

Wer hat den Autovermieter gehackt?

5. Cybercongress

Black Basta

Hinter dem Angriff steht mutmaßlich die Ransomwaregruppe *Black Basta*, die als Nachfolgeorganisation von *Conti* gehandelt wird…

01. **Risiko steigt**

Black Basta hätte es ohne das Know How von Conti nicht geschafft solch ein Unternehmen zu hacken…

02. **Weitere Banden**

Neben Black Basta tauchen nun im wochentakt neue Gruppen, wie u.a. Karakurt oder BlackByte in der Cracker-Szene auf…

5. Cybercongress

Verhandlungen

Ruhe bewahren

Bei den Verhandlungen ist es wichtig ruhig, respektvoll und professionell zu wirken. Emotionen sind in den Verhandlungen fehl am Platz…

Zeit

Mit dem Hinweis, dass es dauert, dass Geld zu organisieren und Bitcoins zu kaufen kann man Zeit gewinnen. In dieser Zeit versuchen wir die Daten irgendwie zu retten.

Schnelligkeit

Anstatt um eine Fristverlängerung zu bitten, kann auch ein geringeres Lösegeld angeboten werden. Es gibt gute Rabatte, wenn man schnell zahlen möchte/kann. Die Kriminellen wollen keine lange Verhandlungen.

Ins Unternehmen

Einbruchstore der Cracker

5. Cybercongress

Platz 1
Mails

59%

Mitarbeiter, die auf eine infizierte E-Mail klicken oder versehentlich Anmeldeinformationen versenden, sind eine der besten Möglichkeiten für Hacker, Zugang zu Ihrem Netzwerk zu erhalten.

59% der erfolgreichen Angriffe erfolgen über eine Mail.

Die richtige Schulung Ihrer Mitarbeiter kann dagegen helfen, deshalb setzen Versicherer auf Awarenessakademien wie z.B. **den Cyber-Fuchs**.

5. Cybercongress

Passwörter

Presse

Passwörter müssen **8 Zeichen lang und komplex** sein (Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Zahlen). Warum? Weil einfache Passwörter einfach zu knacken sind. Ein Passwort mit 8 komplexen Zeichen hat 6,6 Billiarden mögliche Kombinationen.

Ein Hacker könnte niemals jedes einzelne Passwort in seinem Leben ausprobieren.

Realität

Ein Passwort mit 8 Zeichen können innerhalb von 8 Stunden geknacht werden.

Wichtiger als ein langes Passwort ist eher, dass es eine 2FA und unterschiedliche Passwörter je Online-Dienst gibt.

Ansonsten kommen Cracker über die Passwörter z.B. in die Cloud oder in ein Mailpostfach.

5. Cybercongress

Softwarelücken

Veraltete Software

Das betrifft nicht nur Windows, MacOS oder Programme unter den Betriebssystemen sondern immer wieder auch den eigenen Webseiten.

Ein großes Einfallstor sind z.B. Softwarelösungen, die nicht weiter unterstützt werden. Diese werden tw. weiter privat oder beruflich genutzt. Dadurch werden den Kriminellen Tür und Tor in das Unternehmen geöffnet.

5. Cybercongress

Hotspot-Falle

Auf dem Vormarsch

Gefälschte Hotspots sind an sich nichts neues, so können Kriminelle einen Wlan-Hotspot zum Beispiel am Flughafen oder Bahnhof erstellen und so die Opfer auf diesen locken, um an Daten zu kommen.

Nun gibt es Trojaner die einen eigenen Hotspot auf dem verseuchten Laptop eröffnen können, um so an Daten zu gelangen und noch mehr Opfer zu befallen.

Die Kriminellen lassen sich immer wieder etwas einfallen…

Verteilung

Der Angriffe 2022 (CyCo)

01

35%

Ransomware Angriffe im Unternehmen mit & ohne Zahlung

02

25%

Identitätsdiebstahl und Manipulation von MA und Kunden

03

25%

Keine “echten” Incidents, tw. nur Spam-Mails

04

15%

Bunt gemischte Angriffe, wie u.a. verseuchte Webseiten oder Telefonanlagen

5. Cyberkongress

Sicherheitsexperten mahnen an:

Opfer von Cyberangriffen sollen kein Lösegeld zahlen

Eine Gruppe von renommierten IT-Sicherheitsforschenden hat sich in einem offenen Brief an die Bundespolitik dafür eingesetzt, Lösegeldzahlungen nach Angriffen mit Erpresser-Schadsoftware zu unterbinden.

Erpressungstrojaner in Form sogenannter Ransomware seien in den vergangenen Jahren zu einer ernsthaften und dauerhaften Bedrohung für die deutsche und europäische Wirtschaft herangewachsen, heißt es in dem Schreiben, das bereits rund 50 Expertinnen und Experten für IT-Sicherheit und Informatik unterschrieben haben.

5. Cybercongress

Cyber Security

Zusammenfasung

Wegen der hohen Schäden sei die Bereitschaft von Unternehmen, Lösegeld zu zahlen, zuletzt stark gestiegen. "Lösegeldzahlungen sind jedoch bei Ransomware die Wurzel allen Übels",

"Wenn Opfer von Ransomware das geforderte Lösegeld nicht zahlen würden, dann würde dieses Geschäftsmodell im Keim erstickt."

Konkret setzen sich die Forschenden dafür ein, dass Unternehmen die Lösegeldzahlungen nicht mehr von der Steuer absetzen können. Für Unternehmen ab einer bestimmten Größe sollte es eine Meldepflicht für Ransomware-Angriffe und Lösegeldzahlungen geben.

5. Cybercongress

Cyber Security

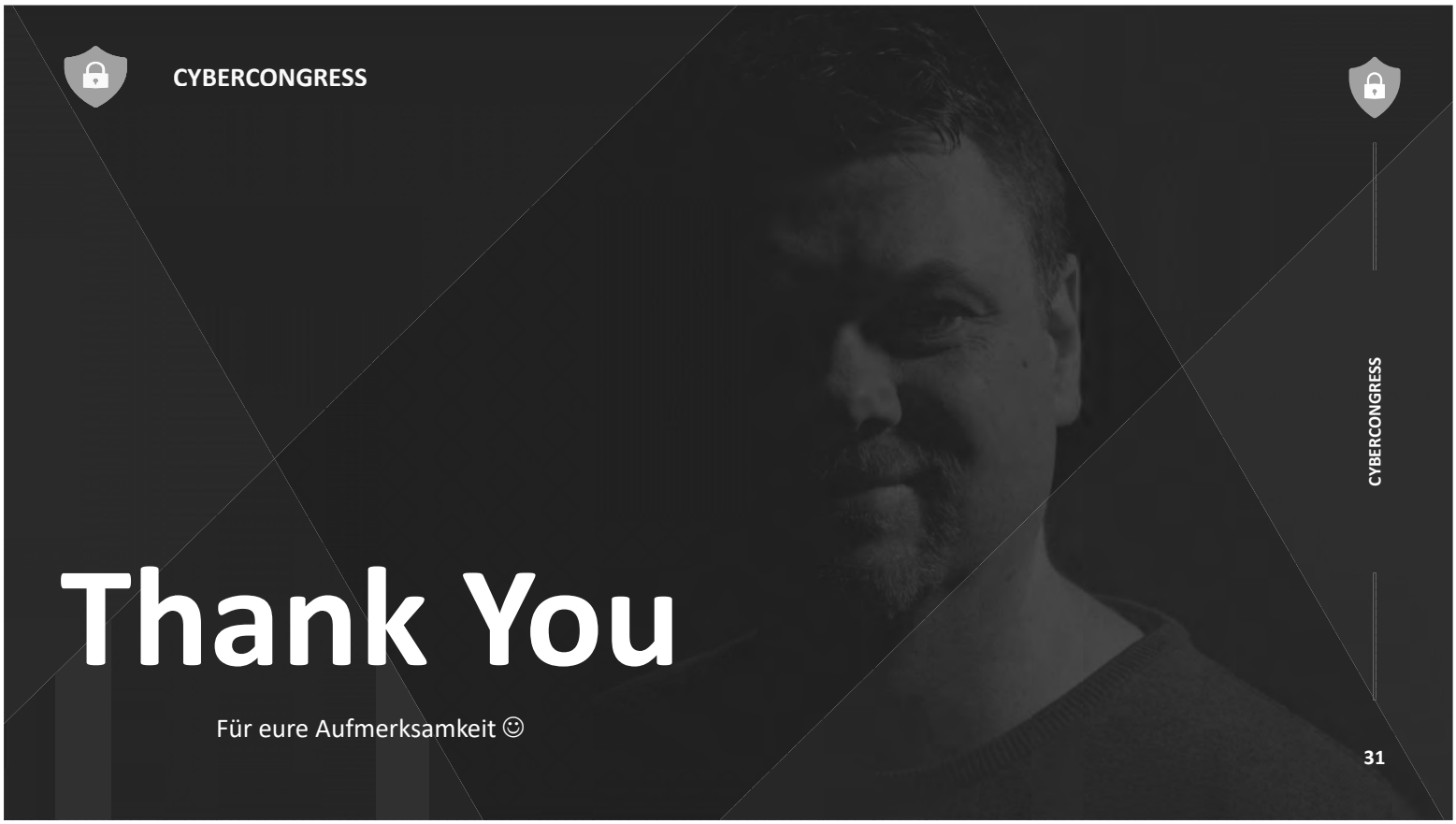
Zusammenfasung

"Da die Versicherer zunehmend starke Sicherheitsmaßnahmen bei den Versicherungsnehmern einfordern, besteht hier die Möglichkeit, die IT-Sicherheit in der Breite signifikant zu erhöhen, ohne weitere regulatorische Maßnahmen treffen zu müssen."

Wenn ein Unternehmen durch Ransomware-Angriffe in eine finanzielle Notlage gerate, sollte der Firma "in angemessener Weise" geholfen werden, beispielsweise über einen Hilfsfonds, so dass diese nicht gezwungen würden, Lösegelder zu zahlen. "Die Unterstützung sollte jedoch an Bedingungen geknüpft sein, welche sicherstellen, dass die Opfer ihre Pflicht zur eigenständigen Absicherung nicht vernachlässigen„.

Was ist grundsätzlich mitversichert?

- Betriebsunterbrechung
- Informationskosten
- Call-Center
- IT-Forensik
- Krisenmanagement
- Haftpflicht
- PR-Beratung
- Kreditkartenüberwachung
- Rechtsberatung
- „Vertrauensschäden“



Thank You

Für eure Aufmerksamkeit ☺

CYBERCONGRESS