Incident Response und IT-Forensik in der Praxis

Thomas Pilz,
Geschäftsführender Gesellschafter Pilz GmbH & Co. KG

30. Cyber-Sicherheitstag
3.Februar 2020
Stuttgart

Gehacked – Was nun?

***Individuen und Interaktion** mehr als Prozesse und Werkzeuge*

***Funktionierende Produkte** mehr als umfassende Dokumentation*

***Zusammenarbeit mit dem Kunden** mehr als Vertragsverhandlung*

***Reagieren auf Veränderung** mehr als das Befolgen eines Plans*

Quelle: Frei nach „Manifest für Agile Softwareentwicklung“, 2001

Cyberangriff: Rückblick, Status und Ausblick – Agile Methoden

Agile@PILZ

***Individuen und Interaktion** mehr als Prozesse und Werkzeuge*

***Funktionierende Produkte** mehr als umfassende Dokumentation*

***Zusammenarbeit mit dem Kunden** mehr als Vertragsverhandlung*

***Reagieren auf Veränderung** mehr als das Befolgen eines Plans*

Quelle: Frei nach „Manifest für Agile Softwareentwicklung“, 2001

Zusammenarbeit mit Security-Experten

- Aber mit Agilen Methoden alleine geht es natürlich nicht, man braucht auch das notwendige Wissen um mit so einer Situation umgehen zu können!
- Daher war es für uns sehr gut, dass wir uns bereits vor dem Angriff mit dem Thema Cybersecurity befasst hatten.
- Dadurch hatten wir bereits Basiswissen im eigenen Unternehmen und konnten reagieren!
- Dadurch hatten wir mit @yet eine auf Cyber Security fokussierte Firma, die mit uns schon vor dem Angriff arbeitete. Leider griffen die Hacker einen Tag vor der Vorstellung der Ergebnisse der Schwachstellenüberprüfung durch @yet an.
- Durch das schnelle Reagieren von Pilz und @yet konnten wir aber dem Angriff schon vom ersten Tag an erfolgreich entgegenwirken
- Leider dauerte es 3 Tage bis wir wussten, dass unsere Polizei der richtige Ansprechpartner ist.
- Unsere Polizei in BW ist beim Thema Cyber Abwehr bestens aufgestellt!
  Ergänzt um die forensische Vorarbeit von @yet konnte die Polizei Ermittlungen aufnehmen, die dazu geführt haben, dass in unserem Fall die Staatsanwaltschaft ermittelt, und deren Ermittlungen bis zum heutigen Tage nicht abgeschlossen sind!

Die Zeit danach

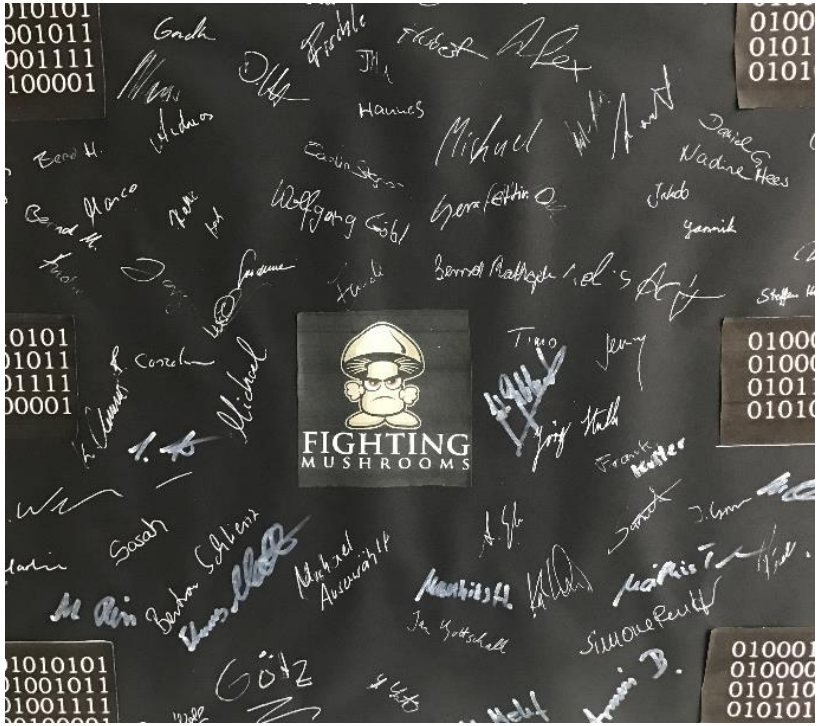
Security als immerwährende Aufgabe der Systemerneuerung

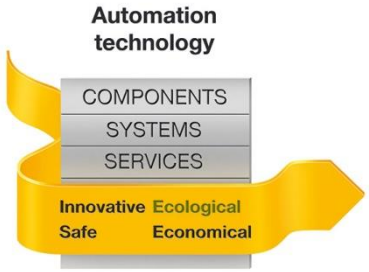
- Wir haben gelernt, dass die Investition in Security Software alleine nicht ausreicht!
- Wir haben gelernt, dass Cyber Abwehr die heute gut ist, in spätestens 3 Jahren veraltet und verwundbar ist!
- Wir haben gelernt, dass die Wirtschaft ein Ziel ist!
- Wir haben gelernt, dass wir uns wehren können!
- Wir haben gelernt, dass wir konstant in die Veränderung und dadurch Verbesserung unserer Securitykonzepte investieren müssen!

Pilz hat die Aufgabe Cyber Security angenommen!

Fazit

Wenn die Securityexperten der Wirtschaft mit den Experten der Polizei zusammenarbeiten, kann man sich erfolgreich gegen Cyberkriminelle wehren!





Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Tel.: +49 711 3409-0

Immer aktuell informiert über Pilz
www.pilz.com

PILZ
THE SPIRIT OF SAFETY