IKARUS Advanced Persistent Threat (APT) Protection mit Sandbox Technologien

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-500 | Fax: +43 1 589 95-100 | office@ikarus.at | www.IKARUS.at | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

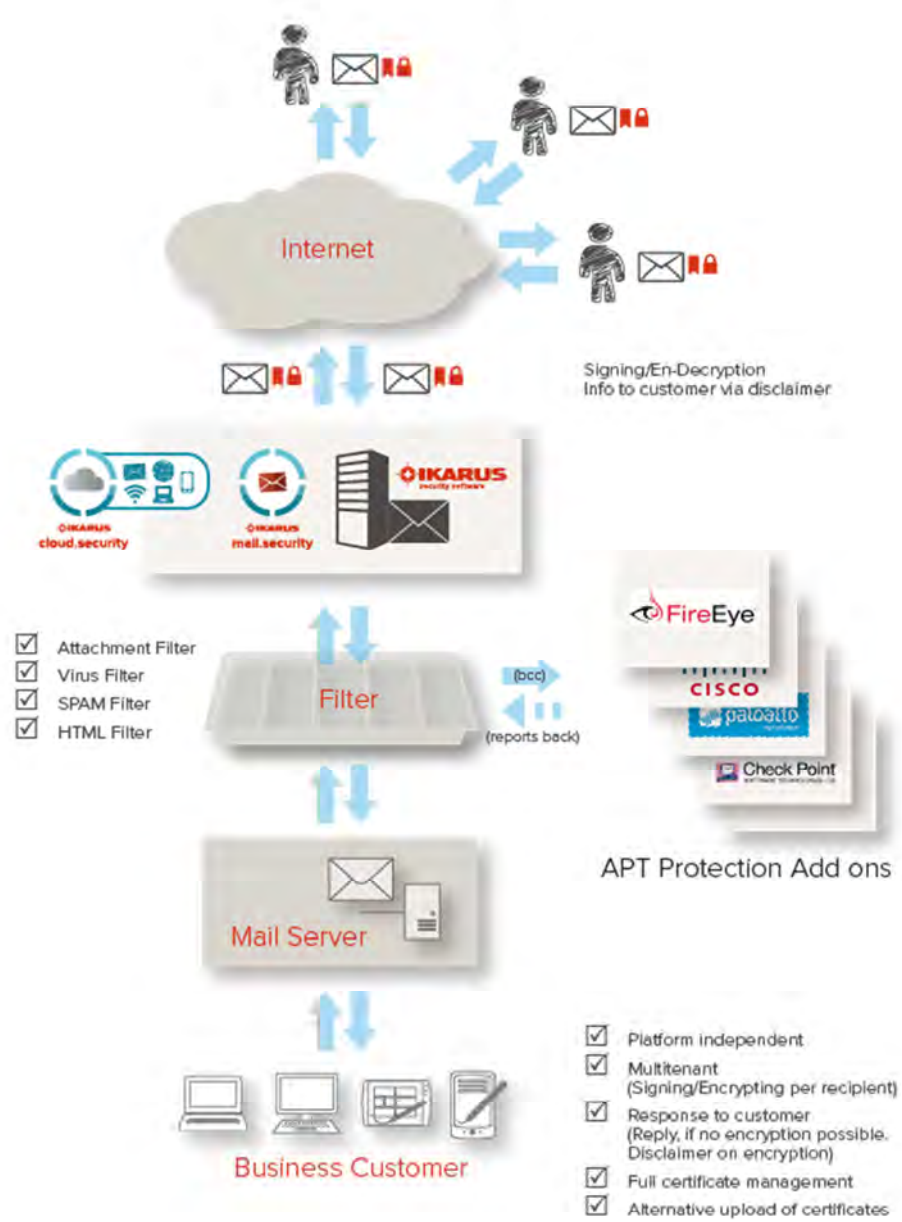
1 Inhaltsverzeichnis

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-500 | Fax: +43 1 589 95-100 | office@ikarus.at | www.IKARUS.at | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

1. Was ist IKARUS APT Protection Add on?

Mehrere SANDBOXes der führenden Hersteller wurden im IKARUS Scan Center in das IKARUS IKARUS mail.security CS integriert.
Das Besondere dran:

- ⇨ (Performance) Nur ein kleiner Teil des gesamten Mailverkehrs wird an die Sandboxes weitergeleitet. Nämlich wenn neue, einzelne und uns noch unbekannte Files kommen, bzw. wenn wir ein Verdacht schöpfen aber nichts in dem Moment in solcher Datei entdecken können.
- ⇨ (Datenschutz) Nur Metadaten werden an die Sandboxes weitergegeben. Eine Weiterleitung der Daten von Sandboxes nach außen wird unterbunden (kein „Telefonieren“ nach Hause)



IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-500 | Fax: +43 1 589 95-100 | office@ikarus.at | www.IKARUS.at | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

2. Wie erkennen wir Malware mit unseren IKARUS ScanEngines?

Der Kern unserer hauseigenen IKARUS Scan Engines bildet die signaturbasierende Erkennung, auch wenn zusätzlich ein Mix aus diversen Technologien wie z.B. Heuristik, Prüfsummen, Gray Listing, Syntax Checks, Foresighted Flags, etc. zum Einsatz kommt.
Ein großer Vorteil: eine sehr hohe Erkennungsrate verbunden mit Schnelligkeit. Stellen Sie sich vor: alleine in unserem IKARUS Scan Center in Wien prüfen wir mit unseren Scan Engines ca. 18 Millionen E-Mails pro Tag, ohne dass die Kunden eine Verzögerung dadurch erfahren. Das bedeutet, dass im Schnitt etwa 208 E-Mails pro Sekunde durch IKARUS mail.security CS geprüft werden.

3. Können wir mit IKARUS mail.security CS 100% Sicherheit garantieren?

100% Sicherheit ist technisch für niemanden machbar und auch wir können das nicht garantieren. An den meisten Tagen lassen wir überhaupt keine Malware durch, aber immer wieder lassen sich die Angreifer gezielt was Neues einfallen, wodurch ein geringer Promillesatz zuerst in der ersten Welle durch unsere Schutzmaßnahme durchrutschen kann. Die Anzahl der nicht erkannten Malware-Mails variiert bei insgesamt von uns geprüften ca. 18 Millionen E-Mail pro Tag zwischen 0 und 300 am Tag.

4. Warum also zusätzlich eine andere Technologie: Sandboxes?

Wie jede Technologie hat auch unser Scan Engine ihre Grenzen. Auch wenn die Anzahl der im mail.security CS ohne Sandbox unerkannten Malware-E-Mails in nur kleinem Promillebereich variiert und mit 0 und ca. 1500 pro Tag im Vergleich zu insgesamt 18 Millionen geprüften E-Mails pro Tag sehr gering ausfällt, ändert sich diese Sichtweise wenn man als Kunde nur ein einziges durchgelassenes E-Mail bekommt und ein Mitarbeiter dieses unglücklicherweise doppelklickt. Daher haben wir nach einer ergänzenden Technologie gesucht, welche uns ermöglicht, auch noch diesen Promillebereich auszumerzen.

Besonders anspruchsvollen und sicherheitsbewussten Kunden können wir dadurch noch mehr Sicherheit bieten.

5. Das Prinzip SANDBOX: wie funktioniert das?

Das Prinzip: Analyse aller Arten von Dateianhängen. Nach einer Anonymisierung werden alle ausführbaren Dateien wie z.B. Executables, Scripts und Makros an die in unserem Scan Center integrierte Sandboxes übergeben, geprüft und das Ergebnis ist direkt über die IKARUS Cloud Security abrufbar.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-500 | Fax: +43 1 589 95-100 | office@ikarus.at | www.IKARUS.at | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

6. Welche Vor- und Nachteile bringen mit sich die beiden Methoden?

Signaturbasierend:

Plus: sehr schnell und genau, auch extrem schnelle Reaktionszeiten auf neue Bedrohungen möglich
Minus ganz neue, gezielte Mail-Angriffe mit Dem Angriffsvektor URL-Links oder so manche obfuscated Scripts lassen sich nicht sofort als Malware erkennen, speziell wenn sie nur vereinzelt und gezielt verschickt werden, auch wenn in der Praxis sich um weniger als 1 Promille handelt

SANDBOX basierend:

Plus: erkennt unter Umständen auch sogar eine einzige auf bestimmten Empfänger zugeschnittene Malware, zum Beispiel bei gezielter APT-Attacke
Minus: bedarf viel Ressourcen und Zeit, gegen so manchen Szenarien machtlos, zum Beispiel wenn ein URL Link in einem Angriffsmail erst nach gewisser Zeit nach dem Versenden mit einer Malware nachträglich scharf gemacht wird

7. Ist einer dieser Ansätze besser?

Nicht unbedingt. Sinnvoll miteinander kombiniert ergänzen sie sich sehr gut und erhöhen um das fehlende Tüpfchen über „i“ die Treffsicherheit unseren Scan Centers

8. Kann man APT Protection Add on zu den bestehenden/ neuen Accounts bestellen?

Ja. Die Freischaltung des Add ons ist sowohl für die neuen als auch für die bestehenden mail.security CS Kunden möglich. Bei laufenden ISC-Accounts bieten wir die Verrechnung der verbleibenden Laufzeit an.

9. Ist ein Test gratis möglich?

Ja. Ein Test für 6 Wochen gratis ist möglich.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-500 | Fax: +43 1 589 95-100 | office@ikarus.at | www.IKARUS.at | Erste Bank Oesterreich | BIC GIBAATWWXXX | IBAN AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405