Monthly Newsletter

November 2021

XAPIENS

Ransomware-As-A-Services dan Bagaimana Cara untuk Mencegahnya

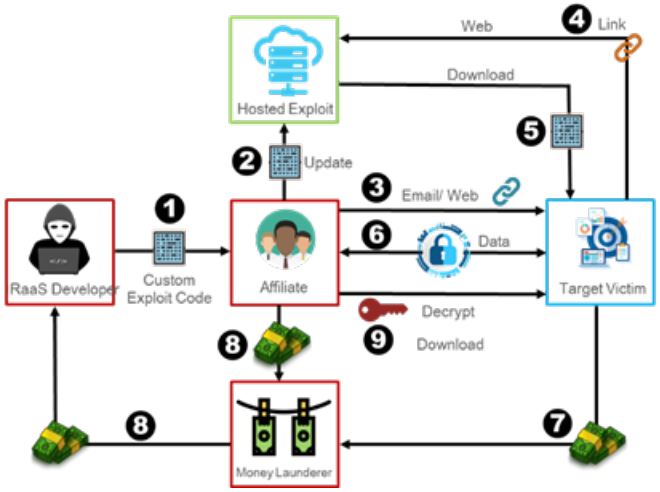
Di era digitalisasi sekarang, dimana penggunaan teknologi yang semakin canggih, keamanan siber (*cyber security*) sudah menjadi suatu hal yang krusial untuk dimiliki oleh organisasi / perusahaan hingga individu. Terutama dalam berinteraksi secara online baik itu menggunakan email, *social media*, ataupun platform lainnya. Meskipun kita memiliki Antivirus ataupun aplikasi pelindung lainnya, bukan berarti kita 100% aman dari ancaman / bahaya *malware*, seperti **Ransomware**. Perlindungan paling baik dari ransomware berasal atau datang dari diri kita sendiri, oleh karena itu penting bagi kita untuk selalu waspada.

img source : uzone.id

Ransomware merupakan jenis *malware* dimana pihak bersangkutan yang menjadi target dan datanya diserang, akan dimintai sejumlah uang sebagai tebusan. Namun terkadang permasalahannya tidak sampai disini saja, apabila target membayar tebusan, mereka kemungkinan bisa menjadi sasaran dari hacker-hacker lain, karena dianggap sebagai *easy target*. Buruknya reputasi perusahaan, kendala dalam produktifitas, kebocoran data, denda, serta adanya biaya investigasi juga menjadi kerugian lain yang dialami perusahaan apabila sudah terserang / terinfeksi Ransomware.

Ransomware as a Service

Ransomware bisa menyerang siapa saja dan kapan saja, baik individu maupun organisasi bisa menjadi targetnya. Yang menjadi tren sekarang adalah munculnya **RaaS (*ransomware as a service*)** yang dapat memperjual-belikan ransomware sehingga orang yang tidak memiliki pengetahuan merancang ransomware pun bisa melakukan serangan ke pihak tertentu (target). Dengan adanya RaaS ini, mempermudah pihak-pihak tidak bertanggung jawab dalam melakukan penyerangan ransomware ke target mereka. Inilah kemudian yang membuat cyber security menjadi semakin krusial untuk kita, terutama dari segi bisnis.



Kasus yang berkaitan dengan ransomware beragam dan terjadi di berbagai negara. Apabila melihat di Indonesia sendiri, salah satu kasus yang pernah terjadi yaitu bocornya data yang diduga dari Indonesia EximBank ke *dark web* pada Maret 2021 lalu. Data yang bocor ini juga tidak bisa dibilang sedikit, dimana diklaim memiliki lebih dari 20 GB data sensitif. Kemudian kasus lainnya, meskipun berasal dari luar negeri, namun dampaknya sampai ke Indonesia adalah serangan ransomware REvil di Kaseya (perusahaan *software* asal Amerika) beberapa waktu lalu. Terdapat beberapa perusahaan yang menjadi pelanggan dari Kaseya di Indonesia yang menjadi target serangan Ransomware. Dimana *software* Antivirus yang dipakai perusahaan tersebut mendeteksi adanya serangan yang muncul.

How to prevent it? Key and Tips

Untuk bisa mengantisipasi hal ini, kita perlu melakukan upaya preventif untuk mencegah perusahaan tempat kita bekerja menjadi korban dari serangan Ransomware. Upaya preventif ini terbagi dalam 3 hal/kategori, yaitu dari sisi **People (SDM), Proses, dan Teknologi**. Apabila kita bisa memperkuat dan mempersiapkan dengan baik SDM, Proses, dan teknologi yang dimiliki perusahaan, pertahanan yang dimiliki dalam menghadapi ancaman ransomware juga semakin baik. Dari sisi SDM, penting bagi perusahaan untuk bisa memiliki karyawan yang memiliki pengetahuan yang baik terhadap *cyber security* dan *cyber threat* diluar sana. Apabila karyawan memiliki pengetahuan akan hal ini, maka mereka juga bisa mengambil langkah pencegahan dan antisipasi yang tepat. Hadirnya training atau seminar cyber security kepada karyawan bisa menjadi salah satu cara bagi perusahaan dalam membekali karyawannya.

Dari sisi teknologi, upaya preventif bisa datang dari bagaimana kita menjaga sistem aplikasi dan jaringan untuk tetap aman. Penting untuk memiliki sistem *Firewall, protection* (untuk email, jaringan, dan lainnya) yang baik sehingga bisa membantu melindungi diri kita dari bahaya ransomware. Sisi teknologi tidak lepas dari sisi proses dimana perusahaan perlu memiliki sistem proses yang baik sebagai bentuk/upaya memperkuat organisasi. Proses ini diantaranya seperti kebijakan, monitoring, audit, dan juga *cybersecurity support*. Pada akhirnya, upaya-upaya yang dilakukan ini bertujuan untuk melindungi data yang kita memiliki. Karena data adalah salah satu asset terpenting yang dimiliki oleh perusahaan dan setiap karyawan mempunyai tanggung jawab untuk bisa menjaga data perusahaan dengan baik.

What Xapiens can Help?

Di Xapiens, *cyber security* merupakan salah satu dari 5 pillar yang dimiliki. Ini karena Xapiens menyadari betapa pentingnya keamanan siber untuk keberlangsungan bisnis serta semakin besarnya ancaman serangan siber. Xapiens memiliki layanan *cyber security* bagi klien yang membutuhkan *support* ataupun mengalami kendala dari sisi *cyber security*-nya. Layanan yang diberikan beragam, mulai dari penetration testing, konsultansi, dan training/pelatihan *cyber security* bagi karyawan di perusahaan. Apabila perusahaan mengalami serangan siber seperti Ransomware, Xapiens Cyber Security juga dapat memberikan bantuan mulai dari *Incident Response, Forensic Check, hingga Security Hardening*.

Xapiens bekerja sama dengan partner yang bergerak di bidang *cyber security* untuk dapat memberikan *service* / Layanan *cyber security* yang baik dan kompetitif di pasaran bagi klien. Dengan **Xapiens Cyber Security**, perusahaan mendapatkan perlindungan dari segi IT Security dan OT security yang dimiliki juga penanganan yang tepat mulai dari pencegahan, analisis, hingga implementasinya. Sekarang pertanyaannya adalah apa yang bisa kami bantu untuk *cyber security* usaha anda?.

(HSP)

Apabila anda tertarik ingin mengkonfirmasi dan mengenal lebih jauh layanan kami, silahkan hubungi **(+62)21 2977 0900** atau email kami di **Hello@xapiens.id**.

References

•NEWS : Terkait Serangan ke Kaseya VSA, Bank dan BUMN Indonesia Juga Ditarget Ransomware REvil (cyberthreat.id)

•NEWS : Hacker Ransomware DarkSide Bocorkan Data Diduga Milik Indonesia EximBank (cyberthreat.id)

Xapiens Cyber Security Catalog

<table>
<tr><th colspan="6">What can we offer?</th></tr>
<tr><th colspan="4">Protection from cyber attack</th><th>Policy Management</th><th>Security Operation</th></tr>
<tr><th>Data Security</th><th>Application Security</th><th>Endpoint Security</th><th colspan="2">Network/Perimeter Security</th><th>Prevention System</th><th>Monitoring and Response</th></tr>
<tr><td>Data Encryption</td><td rowspan="2">Application Architecture</td><td rowspan="2">OT (Operational Technology) EndPoint Protection</td><td rowspan="2">OT (Operational Technology) Network Protection</td><td>Enterprise WiFi Security</td><td>Governance - Policies - Compliance</td><td>Forensic</td></tr>
<tr><td>Data Classification</td><td rowspan="2">Enterprise Firewall / IPS (Prevention) / IDS (Detection)</td><td>Risk Management</td><td>Dark Web</td></tr>
<tr><td>Data Wiping</td><td rowspan="2">Web Application Firewall</td><td rowspan="2">Enterprise End-Point Protection</td><td rowspan="2">OT (operational Technology) Firewall/IPS (intrusion Prevention System)</td><td>Roadmap / Architecture</td><td rowspan="2">Red Team (focused on looking for security gap) and Blue Team (focused on security hardening activities)</td></tr>
<tr><td>Identity Management</td><td>Entreprise web/mail protection</td><td>Training</td></tr>
<tr><td>Public Key Infrastructure</td><td>DevOps Security</td><td>Dekstop Patch Management</td><td rowspan="2">Secured De-militarized Zone (DMZ)</td><td>Network Access Control</td><td>Campaign</td><td>Monitoring and Dashboard</td></tr>
<tr><td>Multi-Factor Authentification</td><td>Cloud Security</td><td>Unified Device Management</td><td rowspan="2">Secure Network Communication / Zero-Trust Network Access and Security Web Gateway</td><td>Penetration testing and Vulnerability Assessment</td><td>Security Operation Center</td></tr>
<tr><td>Backup System</td><td>Multi-Factor Authentification</td><td>Mobile Threat Defense</td><td>AI Surveillance</td><td>Cyberthreat Intelligence</td><td>Security Information and Event Management</td></tr>
</table>