一分（いちぶ）の努力を重ねて、サイバー攻撃に挑む

日本アイ･ビー･エム株式会社
セキュリティー事業本部
セキュリティー･サービス･デリバリー
セキュリティー･シニア･スペシャリスト
X-Force メンバー

戴 開秋
Kaiqiu Dai

日本IBMのERS（エマージェンシー・レスポンス支援サービス）チームに所属する戴開秋は、サイバー攻撃などによるセキュリティー・インシデントに対応するプロフェッショナルだ。サイバー攻撃の標的となってしまった企業から依頼を受け、被害状況の調査や分析を行う。特に最近はサイバー攻撃による被害が相次ぎ、ここ数カ月は毎日のようにセキュリティー・インシデントの調査を行っている状態だ。

「お客様がサイバー攻撃の被害にあわれた場合、その影響範囲がどこまで及んでいるか、徹底的に調査しなければなりません。お客様のシステムのあちこちからログを収集して、どこまで被害が及んでいたかを調査し、報告します。調査が不完全で、例えばウイルスに感染しているパソコンを見落としていると、後でまたお客様が被害を受けることになってしまいます。どこに問題があるか、どう対処すべきなのか、お客様にアドバイスして安心していただけるよう常に意識しています」

ここ数年、企業に対してサイバー攻撃を仕掛けるハッカーたちの動向が、以前とは違ってきていると戴は感じている。従来、ハッカーたちは世界中の様々なシステムに対して、一斉に攻撃を行っていた。しかし、最近では、ハッカーのグループが情報を共有し、互いに連携しながら攻撃を仕掛けていると指摘する。

「いつ、どこのシステムを狙うか、ハッカーたちは情報を共有して攻撃を仕掛けてきます。そうすることで、攻撃が成功する確率を高くしているのでしょう。健康診断の通知を装ったメールが従業員に送られて、添付ファイルを開くとすぐにマルウェアに感染するといった事例もあります。このようにサイバー攻撃の手口は年々、巧妙化しています」

情報を共有し、連携して攻撃してくるハッカーたちにどう対処するか。戴はその答えの一つが、IBMが今年公開した「X-Force Exchange」セキュリティー・インテリジェンス共有プラットフォームにあると言う。

「2013年の国連のサイバー犯行調査結果では、80%の攻撃は、ハッカーたちが情報やツールを共有しながら組織的に行ったものでした。一方、セキュリティー・ソリューションを提供している会社は、自社が持っている情報を他社と共有していません。X-Force Exchangeでは、IBMが約20年にわたって蓄積してきた700テラバイトものセキュリティーに関するデータベースに、誰でもアクセスできるようにしています。これからのサイバー・セキュリティーは、企業間でセキュリティー・インテリジェンスを共有して攻撃に対処する時代になるでしょう」

＊　＊　＊

サイバー・インシデント対応のプロフェッショナルとして最前線で働く戴がセキュリティーに興味を持つよう

セキュリティーの匠

になったのは、セキュリティーとまったく関係のない会社で働いていたときだった。ある日、会社のサーバーがウイルスに感染してしまうという事件が起こる。数日をかけて駆除した経験から、セキュリティーの重要さを身にしみて感じた戴は、そこからセキュリティーについての勉強を重ね、インターネットセキュリティシステムズ社でセキュリティー・コンサルタントとして働くようになる。同社がIBMと統合後もセキュリティーを専門とし、2014年秋から、IBMのセキュリティー研究開発機関「X-Force」のメンバーとしての活動も行っている。

「2014年の夏までIBMのセキュリティー製品のサポート業務をしていて、そこでX-Forceのチームとも長く関係を築いてきました。私がX-Forceのメンバーになったことで、X-Forceの情報提供などのバックアップを受け、ERSにも良い影響が出ていると思います。お客様のセキュリティーに対する意識は、年々高まっており、それにつれて私たちに対する期待も大きくなっているのを感じます。お客様の課題に対して正しいアドバイスができるよう、毎日少しでも新しい知識を身に付けようと意識しています」

戴の座右の銘は、中学生の時に出会った「一分(いちぶ)の努力に一分の収穫、努力なくして収穫なし、努力は遅かれ早かれ必ず報われる」という言葉だ。

「この言葉を思い出すと、リラックスできるのです。結果が出なくても、努力していればいつか報われるだろうと思えて気持ちが落ち着きます。今の自分があるのも、がんばって努力を続けてきたから。努力しないと収穫は何もないけど、努力をすれば多かれ少なかれ収穫があるはず。そう思うと、努力することが辛くなくなります」

＊　＊　＊

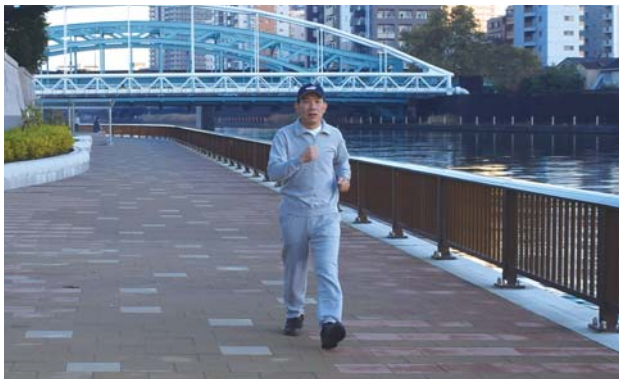
高度化・巧妙化する最近のサイバー攻撃から企業を完全に守ることには限界がある。戴は万が一インシデントが起きてしまった場合を想定した対策も必要だという。

「従業員の教育も欠かせないし、新しいセキュリティー・ソリューションを導入することも大切でしょう。その上で、感染してしまった場合、いかにすばやく検知して、被害を広めないための作業を行うかが非常に重要です。インシデントが発生した際、その原因や影響範囲を調査する組織CSIRT(Computer Security Incident Response Team)を自社内に作ることを検討されているお客様も多く、CSIRTの構築を支援してほしいというリクエストも度々いただくようになりました。こうした傾向は、今後も続いていくのではないでしょうか」

＊　＊　＊

最近の日課は、1万歩を歩くこと。仕事から帰って歩数が足りない時は、1万歩になるまで家の中を何往復も歩きまわる。この生真面目さこそが戴の個性であり、サイバー・インシデント対応のプロフェッショナルにはそれぐらいの生真面目さが必要なのかもしれない。

「大学時代には友達とよくサッカーをしていましたが、ポジションはディフェンダー(笑)。攻撃よりも守ることの方が自分の性に合っているのだと思います」



よく歩くのは、家の近くの川沿いの道。約1時間歩いても、1万歩にはまだ届かない…。

X-Forceのアトランタ本部で、X-Force QAチーム シニア・ソフトウェア・エンジニアのNatthapol Prakongpanと。