DAS KANN ALLEN FIRMEN PASSIEREN

Interview: Christian Rühmkorf

CYBERANGRIFF AUF DAS UNTERNEHMEN PARABEL

MŮŽE SE TO STÁT KAŽDÉ FIRMĚ

KYBERNETICKÝ ÚTOK NA FIRMU PARABEL

Nahezu 9 von 10 Unternehmen sind von Cyberangriffen betroffen. Das ist das Ergebnis einer repräsentativen Studie des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen befragt wurden. Dieses Schicksal hat auch das Unternehmen Parabel ereilt. Parabel bietet Entwicklung und Konstruktion im Bereich Maschinenbau, Anlagenbau und Automotive. Wir sprachen mit dem Geschäftsführer Michael Krüsselin und seinem IT-Experten Jaromír Grác über den Hackerangriff, den das Unternehmen mit einem blauen Auge überstand.

Skoro 9 z 10 společností je ohroženo kybernetickými útoky. Vyplývá to z reprezentativní studie německého svazu digitálních technologií Bitkom, na které se podílelo více než 1000 firem ze všech odvětví. Svou zkušenost má i Parabel. Firma, která pro výrobce strojů a zařízení a automobilový průmysl vyvíjí a vyrábí technické produkty. O hackerském útoku, ze kterého Parabel nakonec vyvázl v podstatě se zdravou kůží, jsme hovořili s jeho ředitelem Michaelem Krüsselinem a IT specialistou Jaromírem Grácem.

Wann und wie haben Sie gemerkt, dass etwas nicht stimmt?

Grác: Gleich am Morgen, kurz vor 7 Uhr meldeten meine Kollegen, dass unser SAP-System nicht funktioniert. Ich bin sofort zur Arbeit, habe die Server gecheckt und versucht, mich im SAP-System anzumelden. Die Server waren online, aber beim SAP kam eine Fehlermeldung. Ich konnte mich auch nicht als Administrator beim SAP-Server anmelden. Es war gleich klar, dass es sich um ein Problem in der ganzen Firma handelt, nicht nur bei einzelnen Mitarbeitern. Auch der Neustart der Server hat nichts gebracht. Dann habe ich noch auf dem Server die Logs im Windows geprüft, ob es da z.B. zu einer Aktualisierung am Abend kam, was aber nicht der Fall war. Mehr konnte ich zu dem Zeitpunkt nicht machen. Also habe ich das Problem der Firma ABIA gemeldet, die unser SAP-System verwaltet. Nach ein bis zwei Stunden stand fest, dass unser SAP-System beschädigt ist, einige Daten sogar gelöscht und Dienste beschädigt wurden und es wahrscheinlich zu einem Hacker-Angriff kam. Ich sollte mich an die Firma NWT wenden, die unsere Server verwaltet.

Kdy a jak jste zjistili, že něco není v pořádku?

Grác: Hned ráno, krátce před sedmou, mi kolegové hlásili, že nefunguje SAP. Okamžitě jsem jel do práce, zkontroloval servery a zkusil se do SAPu přihlásit. Servery byly online, ale SAP hlásil chybu. Na server SAP jsem se nemohl přihlásit ani jako administrátor. Okamžitě mi bylo jasné, že máme problém v celé firmě, nejen u jednotlivých zaměstnanců. Zkusil jsem restartovat server, ale ani to nepomohlo. Potom jsem ještě na serveru zkontroloval protokoly ve Windows, chtěl jsem zjistit, jestli například večer proběhla aktualizace, ta ale neproběhla. To bylo vše, co jsem v tu chvíli mohl dělat. Nahlásil jsem problém firmě ABIA, která nám spravuje SAP. Asi za hodinu nebo dvě bylo jasné, že náš SAP je poškozen, některá data byla smazána a některé služby poškozeny a pravděpodobně došlo k hackerskému útoku. Kontaktoval jsem tedy firmu NWT, která nám spravuje servery.

Was konnte die Firma über den Hackerangriff sagen?

Grác: Sie hat festgestellt, dass seit zwei Tagen ein unbekannter „Gast" den Server beobachtete. Er hatte es auf das SAP-System abgesehen, installierte Hackerprogramme und Skripte und versuchte, die Backups des Servers zu zerstören. Darüber hinaus versuchte er den ganzen SAP-Server zu chiffrieren, aber unser Antivirenprogramm konnte das verhindern, der Hacker konnte es nicht deinstallieren. Die Firma NWT erstellte daher eine Sicherungskopie des SAP-Servers für weitere Untersuchungen und stellte die vorherige Version des Servers wieder her, bevor der Server angegriffen wurde. Die Wiederherstellung dauerte dank der Backup-Technologie nur 30 Minuten, viel länger dauerte die Überprüfung des SAP-Servers und der gesamten Umgebung, um herauszufinden, ob der Angreifer auf weitere Geräte oder Server zugegriffen hatte.

Co jste se od nich o hackerském útoku dozvěděl?

Grác: Tam zjistili, že náš server už dva dny sledoval neznámý „host". Zaměřil se na SAP, nahrál na něj hackerské programy a skripty a pokusil se zničit zálohy serveru. Dále zkusil server SAP zašifrovat, tomu ale zabránil náš antivirový program, hacker ho nedokázal odinstalovat. Firma NWT zálohovala server SAP pro další šetření a obnovila verzi serveru před útokem. Díky zálohovací technologii obnova trvala asi půl hodiny, mnohem více času zabrala kontrola serveru SAP a celého prostředí. Bylo potřeba zjistit, jestli se útočník nedostal i na další zařízení nebo servery.

Das heißt, der Hacker wollte Ihre Daten blockieren oder entfremden und Lösegeld erpressen?

Krüsselin: Ja, wahrscheinlich hätte er das gemacht, wenn wir die Daten verloren hätten. Wir haben Gott sei Dank im SAP keine Daten verloren, weil wir ein Backup vom letzten Tag hatten. Die Antivirus-Software, die uns vor Schlimmerem bewahrt hat, haben wir vor nicht einmal einem halben Jahr gekauft. Die Polizei meint, bei Firmen, die ähnliche Angriffe hatten, habe das Antivirussystem, was wir vorher hatten, nicht geholfen.

Takže hacker chtěl zablokovat nebo odcizit vaše data a potom vymáhat výkupné?

Krüsselin: Ano, kdybychom o data přišli, pravděpodobně by to udělal. Naštěstí jsme žádná data v SAPu neztratili, měli jsme zálohu z předchozího dne. Ani ne před půl rokem jsme si pořídili nový antivirový software a ten nás zachránil před nejhorším. Policie nám řekla, že firmy, které zažily podobné útoky a měly ten samý antivirus jako původně my, ochráněny nebyly.

Mit anderen Worten, Sie sind mit einem blauen Auge davongekommen.

Krüsselin: Erstmal ja.

Das freut uns. Wie solche Angriffe ablaufen und wie man sich besser schützen kann, sind ganz wichtige Infos für unsere Mitgliedsunternehmen. Ganz sicher macht es Sinn, ein Cybersecurity-Audit machen zu lassen, oder?

Krüsselin: Genau. Durch die Erfahrungen der anderen haben wir uns vor einiger Zeit intensiver mit dem Thema beschäftigt und deshalb auch abgesichert. Das hat uns geholfen. Wie Sie sagen, mit einem blauen Auge davongekommen.

Können Sie den Schaden ungefähr beziffern?

Krüsselin: Die Kosten für die Wartung und den Service betrugen ungefähr 50 000 Kronen. Und wir haben anderthalb Tage nicht im SAP arbeiten können. Wir konnten keine Angebote verschicken, keine Rechnungen ausstellen, keine Bestellungen bearbeiten. Diesen Schaden können wir nicht abschätzen.

Haben Sie eine Idee, wie dieser Gast auf den Server gekommen ist? Kann ein eigener Mitarbeiter dafür verantwortlich gewesen sein, absichtlich oder nicht absichtlich? Home-Office steht manchmal in der Kritik, weil die VPN-Verbindung zum Beispiel ein Einfallstor für Hacker sein kann.

Grác: Schwer zu sagen. Der Angriff kann zum Beispiel über unzureichend gesicherte Dienste erfolgen, über ein Kamera-System, über ein Handy. Heute hat jeder Mitarbeiter ein Handy mit mobilen Daten. Das kann gehackt werden, wenn die Mitarbeiter im öffentlichen Netz sind. Plötzlich hat man ein infiziertes Gerät im Firmennetz und sofort entsteht ein Loch im System. Der Hacker kann sich Zugang zum Intranet verschaffen und diesen Zugang missbrauchen. Wir wissen nur, dass die IP-Adresse, über die der Angriff gelaufen ist, aus dem Ausland war. Komplette Informationen über die Logs etc. kann nur unser Internetanbieter an die Polizei übergeben. Wir müssen abwarten, was die Polizei herausfindet.

Jinými slovy – vyvázli jste z toho se zdravou kůží.

Krüsselin: Prozatím ano.

To jsme rádi. Jak takové útoky probíhají a jak se před nimi můžeme chránit, to jsou pro naše členy velmi důležité informace. Určitě je potřeba udělat audit kybernetické bezpečnosti.

Krüsselin: Přesně tak. Věděli jsme, jaké zkušenosti měli ostatní, a proto jsme se před časem začali tímto tématem intenzivněji zabývat a lépe jsme se zabezpečili. To nás zachránilo. Jak říkáte, vyvázli jsme se zdravou kůží.

„O všem se příliš mnoho mluví a málo koná."

„Es wird einfach zu viel über alles geredet und zu wenig gehandelt."

Můžete vyčíslit přibližnou škodu?

Krüsselin: Údržba a servis nás stály asi 50 000 korun. Kromě toho jsme jeden a půl dne nemohli pracovat v SAPu. To znamená, že jsme nemohli posílat nabídky, nemohli jsme vystavovat faktury, nemohli jsme zpracovávat objednávky. Tyto škody odhadnout nemůžeme.

Máte nějakou představu, jak se ten nezvaný host na váš server dostal? Mohl za to někdo z vašich zaměstnanců, ať už úmyslně, nebo neúmyslně? Občas se kritizuje home office, protože například připojení přes VPN může být vstupní branou pro hackery.

Was glauben Sie, warum ist gerade Ihre Firma Parabel ins Visier geraten? Oder machen die Hacker das wie die Kühe - grasen einfach alles ab?

Krüsselin: Ich denke, es kann allen Firmen passieren. Es war wahrscheinlich ein globaler Angriff, sie haben interessante Adressen und ihre Schwächen gesucht. Die Polizei hat gesagt, dass zu dieser Zeit auch andere Firmen ähnliche Angriffe gemeldet haben. Sie meinen, es handle sich um eine organisierte Gruppe.

Von wem erwarten Sie jetzt Schritte, die das künftig verhindern könnten? Muss SAP irgendetwas ändern, muss jede Firma selber etwas machen? Erwarten Sie Hilfe vom Staat?

Krüsselin: Wir wünschen uns schon Hilfe, aber glauben nicht, dass sich etwas tun wird. Es wird einfach zu viel über alles geredet und zu wenig gehandelt. Unser Unternehmen ist jetzt 25 Jahre alt. Von öffentlicher Seite wurde uns nie geholfen. Wir haben uns immer selber geholfen und werden das auch in Zukunft so machen. Es geht nicht anders.

Was könnte die öffentliche Hand tun, damit sich was ändert?

Krüsselin: Auf jeden Fall strafrechtlich restriktiver vorgehen, die Strafen verschärfen. Vielleicht sollte auch die Polizei in diesem Bereich ihre Aktivitäten verstärken. Das Problem ist komplex, es betrifft nicht nur Firmen, sondern auch Privatpersonen.

Grác: Těžko říct. Útok může probíhat například přes nedostatečně zabezpečené služby, přes kamerový systém, přes mobilní telefon. Dneska má každý zaměstnanec mobilní telefon s mobilními daty. Když je ve veřejné síti, může ho napadnout hacker. A najednou máte ve firemní síti infikované zařízení a v systému je okamžitě díra. Hacker může získat přístup do interní sítě a zneužít ho. Jediné, co víme, je, že IP adresa, ze které došlo k útoku, byla ze zahraničí. Kompletní informace o protokolech atd. může policii předat pouze náš poskytovatel internetu. Musíme tedy počkat, co policie zjistí.

Proč si myslíte, že se terčem útoku stal právě Parabel? Nebo se hackeři chovají tak nějak jako krávy – spasou všechno, co mají kolem sebe?

Krüsselin: Myslím, že se to může stát každé firmě. Pravděpodobně šlo o globální útok, hackeři hledali zajímavé adresy a jejich slabiny. Policie nám řekla, že v té době došlo k podobným útokům i na další firmy. Jsou toho názoru, že je to organizovaná skupina.

Co myslíte, kdo by teď měl podniknout nějaké kroky k tomu, aby se to v budoucnu neopakovalo? Musí něco změnit SAP, musí se o to postarat firmy samy? Očekáváte, že vám pomůže stát?

Krüsselin: Přáli bychom si, aby nám stát pomohl, ale nevěříme, že to udělá. O všem se příliš mnoho mluví a málo koná. Naší firmě je letos 25 let. Pomoci od státu jsme se nikdy nedočkali. Vždycky jsme si pomáhali sami a tak tomu bude i v budoucnu. Jinak to nejde.

Co by mohl udělat veřejný sektor?

Krüsselin: V každém případě by měl postupovat restriktivněji v oblasti trestního práva, zpřísnit tresty. Možná by i policie měla být v této oblasti aktivnější. Je to komplexní problém, netýká se jenom firem, ale i soukromých osob, každého z nás.