BLEIBEN SIE DEN ANGREIFERN IMMER EINEN SCHRITT VORAUS

Ein Sicherheitsleitfaden
zu effektiver Cyberabwehr

F-Secure

SO SCHÜTZEN SIE IHR UNTERNEHMEN VOR SICHERHEITSVORFÄLLEN

Datenlecks und Datenschutzverstöße zu unterbinden, hat für jedes Unternehmen Priorität. Der Verlust vertraulicher Informationen, etwa von geistigem Eigentum oder von Kundendaten, kann Ihr Unternehmen zerstören und die Privatsphäre Ihrer Kunden gefährden. Leider können Sie sich nicht darauf verlassen, dass Sie alle Bedrohungen abfangen können, bevor sie in die Infrastruktur gelangen.

Darum ist die Schnelligkeit der Erkennung ein zentraler Punkt. Ein typischer Cyberangriff verläuft in mehreren Phasen, und es kann Monate oder Jahre dauern, bis er abgechlossen wird. In jeder Phase kann der Verteidiger die Aktionen des Angreifers durch verschiedene Maßnahmen, die in diesem Handbuch behandelt werden, behindern oder stoppen. Je früher in der Cyber Kill Chain ein Eindringling entdeckt wird, desto weniger Schäden entstehen und desto geringer sind die Folgekosten von Sicherheitsvorfällen.

Unser eBook **„Der dunklen Seite einen Schritt voraus“** beschreibt ein Sicherheitsszenario bei einem großen Fertigungsunternehmen. Diese fiktive Geschichte nimmt ein schlimmes Ende. Mit ein paar grundlegenden Sicherheitsmaßnahmen hätten aber viele der unglücklichen Folgen verhindert werden können.

Dieser Leitfaden stellt wirksame Gegenmaßnahmen vor, die alle Organisationen gegen Angreifer einsetzen können. Er gibt praktische Tipps zur Resilienz-verbesserung bei Cyberangriffen und zur Erkennung von Bedrohungen.

In der Welt der Cybersicherheit sind Sie ein leichtes Ziel, wenn Sie nicht ständig in Bewegung bleiben.

Lesen Sie unser eBook.

> „Der dunklen Seite einen Schritt voraus“ schildert den Kampf zwischen Pulp Global, einem globalen Fertigungs-unternehmen, und Number One, einem kriminellen Hacker, der Teil einer organisier-ten kriminellen Vereinigung ist.

“ Als das Projekt von Pulp Global wiederholt in den Nachrichten auftauchte, beschloss Number One, die Gelegenheit zu nutzen. Die Gruppe wollte prüfen, wie stark die Cybersicherheit des Unternehmens war und ob dort Geld zu holen sei.

Number One nimmt sich Pulp Global als Ziel für einen Cyberangriff; eBook „Der dunklen Seite einen Schritt voraus“

VERTEIDIGUNGSTAKTIK 1: ÖFFENTLICHE VON INTERNEN INFORMATIONEN TRENNEN

Zu Beginn eines gezielten Angriffs ist der Angreifer immer im Vorteil. Verteidiger haben kaum Möglichkeiten, zu erfahren, ob und wie sie angegriffen werden, und meist keine Ahnung, dass Angreifer bereits Intrusionsstrategien testen. Es gibt aber Taktiken, diese Versuche erheblich zu erschweren.

Angreifer nutzen sowohl öffentlich verfügbare als auch heimlich beschaffte Informationen. Selbst scheinbar Irrelevantes kann für einen Angreifer wertvoll sein, beispielsweise ein Gespräch beim Mittagessen, ein Foto in den sozialen Medien oder eine Referenzgeschichte auf Ihrer Website.

Es ist wichtig, klare Grenzen zwischen internen und externen Informationen zu ziehen. Stellen Sie sicher, dass Ihre Mitarbeiter wissen, was sie nach außen teilen dürfen und was nicht. Legen Sie eine Klassifikationsrichtlinie fest, um sicherzustellen, dass Ihre Daten ordnungsgemäß gekennzeichnet und gehandhabt werden.

"Number One und sein Team begannen, so viele Informationen wie möglich über Pulp Global aus verschiedenen frei verfügbaren Quellen wie Nachrichtenartikeln und Pressemitteilungen zu sammeln. Dies umfasste Informationen über Anbieter und Zulieferer, Wartungsunternehmen, Mitarbeiter in Schlüsselpositionen und Informationen über die IT- und OT-Systeme. In den gesammelten Daten und Informationen tauchte stets eine Fabrik auf: Segnen.

Aufgrund der Menge an verfügbaren Informationen entschied sich Number One dafür, sich auf die Fabrik in Segnen zu konzentrieren. Der Plan war, Segnen zum ersten Einstiegspunkt zu machen.

Die Recherche- und Sondierungsphase des Angriffs von Number One auf Pulp Global; eBook „Der dunklen Seite einen Schritt voraus"

VERTEIDIGUNGSTAKTIK 2: DIE SICHERHEITS-KULTUR IM UNTERNEHMEN FÖRDERN

Die Aktionen eines Cyberangreifers können sehr glaubwürdig erscheinen und auf jeden einzelnen in der Firma abzielen. Aus diesem Grund ist die Schulung der Mitarbeiter zum Thema Sicherheit von entscheidender Bedeutung.

Wissen Ihre Mitarbeiter, wie sie entscheiden sollen, ob sie auf einen Link klicken dürfen oder nicht? Verwenden sie ein einzigartiges Kennwort für jeden verwendeten Dienst? Verwenden sie ihre geschäftliche E-Mail-Adresse und ihr Passwort, um auf persönliche Dienste zuzugreifen? Grundlegende Sicherheitsmaßnahmen sollten im Bewusstsein aller Mitarbeiter fest verankert sein. Alle sollten so geschult sein, dass sie Phishing-E-Mails erkennen und auf ihre Surfgewohnheiten im Internet achten.

Security-Awareness-Schulungen müssen ansprechend und einprägsam gestaltet werden, um effektiv zu sein. Geben Sie Ihren Mitarbeitern Mittel an die Hand, wie sie mögliche Angriffe erkennen. Lassen Sie sie wissen, welche Rolle sie für die Datensicherheit spielen. Damit Ihre Mitarbeiter sich der Sicherheitsaspekte stets bewusst sind, sollten Sie das Schulungsprogramm zu einem fortlaufenden Prozess machen. Fördern Sie das Sicherheitsverhalten Ihrer Mitarbeiter, indem Sie bei Bewusstsein, Einstellung und Wissen ansetzen.

THEMEN FÜR SICHERHEITSTRAININGS

Phishing

Phishing-Versuche erkennen und das Verhalten bei verdächtigen Links sowie gefälschten Internet-Login-Seiten üben.

Drahtlose Netzwerke

Wie drahtlose Netzwerke funktionieren und welche Risiken man beim Herstellen einer Verbindung zu unbekannten Netzwerken eingeht.

Physische Sicherheit

Warum es wichtig ist, Schreibtischschubladen und Computer abzuschließen, vertrauliche Dokumente zu vernichten, Ausweise zu verlangen und die Identität unbekannter Bürogäste zu prüfen.

Passwortsicherheit

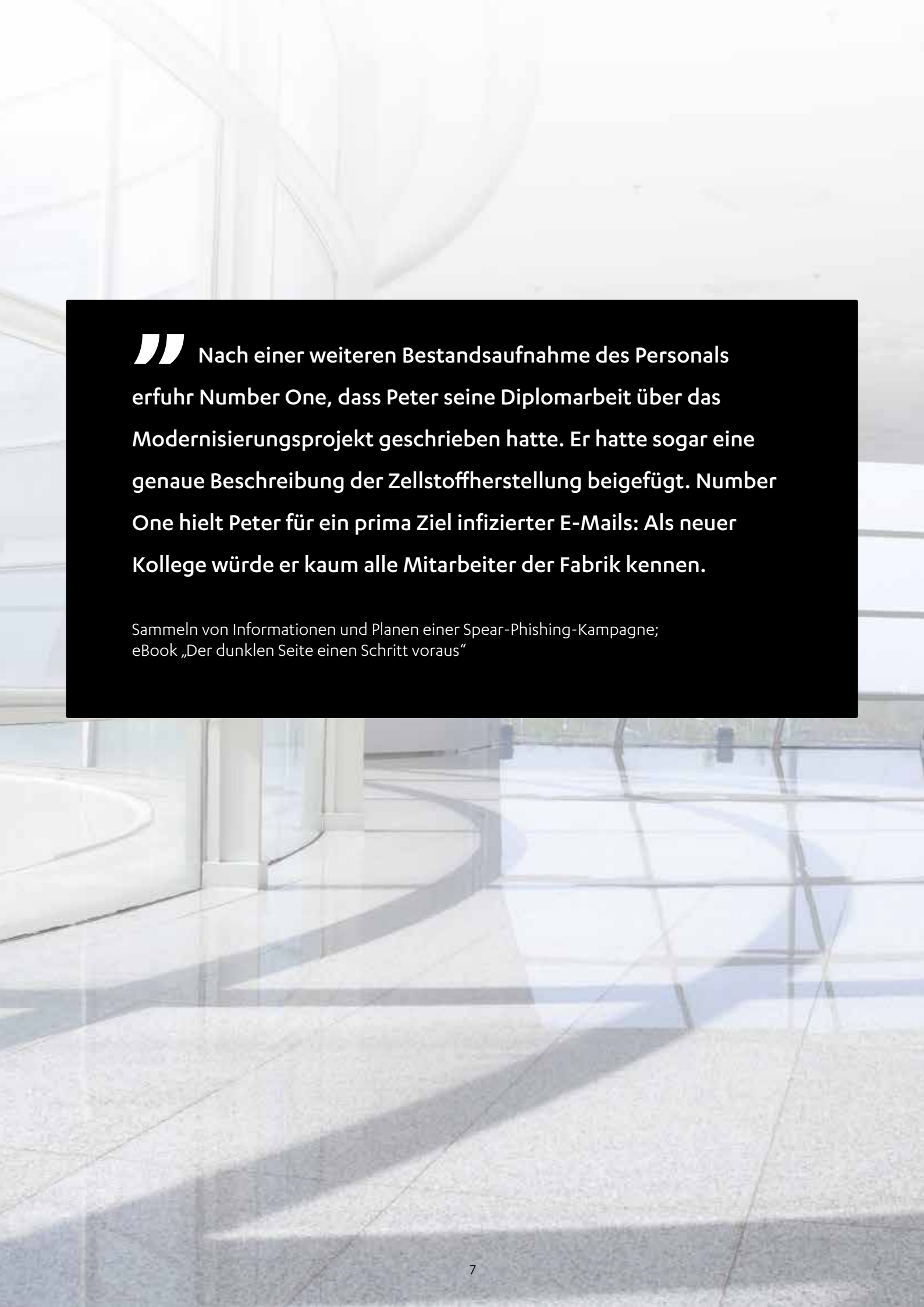
Sichere Methoden zur Verwendung und Verwaltung von Passwörtern und über die Risiken von Mehrfachverwendung, leicht zu erratenden und ungeänderten Passwörtern sowie der arglosen Weitergabe.

Desktop-Sicherheit

Welche Folgen es haben kann, wenn Computer nicht gesperrt oder ausgeschaltet werden und wenn unbekannte Geräte einfach angesteckt werden.

Malware

Wie man Malware erkennen kann und was zu tun ist, wenn ein Benutzer den Verdacht hat, dass sein Gerät infiziert ist.



> **Nach einer weiteren Bestandsaufnahme des Personals erfuhr Number One, dass Peter seine Diplomarbeit über das Modernisierungsprojekt geschrieben hatte. Er hatte sogar eine genaue Beschreibung der Zellstoffherstellung beigefügt. Number One hielt Peter für ein prima Ziel infizierter E-Mails: Als neuer Kollege würde er kaum alle Mitarbeiter der Fabrik kennen.**

Sammeln von Informationen und Planen einer Spear-Phishing-Kampagne;
eBook „Der dunklen Seite einen Schritt voraus“

VERTEIDIGUNGSTAKTIK 3: CYBERRISIKEN MODELLIEREN UND QUANTIFIZIEREN

Sich beizeiten auf Cyberbedrohungen einzustellen, kann einen großen Unterschied machen, wenn es darum geht, wie schnell ein Unternehmen reagieren und sich wieder erholen kann. Eine angemessene Risikobewertung ist eine Aufgabe für ein übergreifendes Team, das viele Funktionen innerhalb Ihres Unternehmens sowie relevante Drittparteien umfasst.

Ein solides Sicherheitsprotokoll beginnt mit der Ermittlung dessen, was geschützt werden muss. Anschließend gehen Sie mit dem Team ins Brainstorming und eruieren Risiken, Schwachstellen und Bedrohungsakteure. Sie können die Zukunft zwar nicht vorhersagen, aber Sie können eine gute Ausgangsposition schaffen. Erstellen Sie Risikoprognosen, machen Sie eine Bestandsaufnahme potenzieller Angreifer und Ihrer eigenen Schwachstellen. Entwickeln Sie detaillierte Bedrohungsszenarien – oder Geschichten über Angreifer –, die die Ergebnisse in die Realität holen. Sobald Sie sich ein schlüssiges Bild gemacht haben, können Sie die Risiken überprüfen und quantifizieren. Und ermitteln Sie deren Kosten! Erst dann können Sie fundierte Entscheidungen treffen und die Ausgaben für Cybersicherheit rechtfertigen.

Führen Sie zuletzt Tests durch. Stellen Sie Ihre Verteidigung selbst auf den Prüfstand oder beauftragen Sie ein „Red Team" damit, einen Angriff zu simulieren. Ananalysieren Sie die Ergebnisse und starten Sie den ganzen Prozess von vorne.

> „Martin war überfordert. Pulp Global hatte keine Pläne oder Verfahren, um ihn bei einem Cybervorfall zu unterstützen. Es gab keine festgelegten Prozesse oder Richtlinien und keine internen oder externen Kommunikationspläne. Es kamen Fragen vom Vorstand, den Mitarbeitern, seinem IT-Team und von Reportern – Fragen, die er nicht beantworten konnte. Da er keine Erfahrung im Umgang mit einem Cybervorfall hatte, war der CIO schlichtweg überfordert.
>
> Martin wusste, dass er externe Hilfe hinzuziehen musste, um die Situation zu bewältigen. Er bat die Lieferanten, die die Fabrik in Segnen belieferten, sofort Ersthelfer dorthin zu schicken.
>
> Pulp Global wurde überrascht, da man keine Vorfallszenarien getestet hatte;
> eBook „Der dunklen Seite einen Schritt voraus"

VERTEIDIGUNGSTAKTIK 4: ENDGERÄTE-SCHUTZ GEGEN COMMODITY-MALWARE

Gezielte Angriffe ziehen viel Aufmerksamkeit auf sich. Die meisten Bedrohungen sind jedoch Commodity-Bedrohungen: Massenmalware, Ransomware, Spam und häufige Exploits. Diese sind nicht unbedingt auf dem neuesten Stand der Technik, aber sie sind wirksam gegen Systeme, die nicht gepatcht sind oder keinen effektiven Endgeräteschutz haben.

Commodity-Bedrohungen machen den größten Anteil der sicherheitsbezogenen Kosten eines Unternehmens auf – sowohl in Bezug auf die Zeit als auch auf die Produktivität. Aus diesem Grund sollte der Endgeräteschutz das Fundament der Sicherheitsstrategie bilden.

Sie können mit relativer Leichtigkeit die meisten Bedrohungen verhindern und eine gesunde „Sicherheitshygiene" erreichen. Mit den richtigen grundlegenden Sicherheitspraktiken können Sie sogar hochentwickelten Angreifern das Leben schwer machen. Warum sollten Sie ihnen den roten Teppich ausrollen?

Informieren Sie sich darum über eine umfassende EPP-Lösung (Endpoint Protection), die all Ihre Geräte abdeckt, von Windows-Computern und Macs bis hin zu iOS- und Android-Geräten.

ENDGERÄTESCHUTZFUNKTIONEN, NACH DENEN SIE AUSSCHAU HALTEN SOLLTEN

Zentrale Verwaltung

Sicherheitsfunktionen auf allen Geräten in einem Schritt bereitstellen und über ein Portal verwalten.

Ransomware-Schutz

Das Unternehmen gegen Ransomware härten und Daten im Falle eines Angriffs wiederherstellen.

Bewährte Schutzfunktionen

Gute Testergebnisse von vertrauenswürdigen Vergeichs- und Prüfinstituten.

Mobiles VPN

Man-in-the-Middle-Angriffe unterbinden und auch aus unsicheren WLAN-Netzwerken heraus sicher arbeiten.

Patch-Management und Mobile-Device-Management

Sicherheitslücken in Software automatisch beheben und Mobilgeräte kontrolliert einbinden.

RANSOMWARE

Schadsoftware, die Fehlfunktionen bewirkt oder Daten verschlüsselt, um Geld zu erpressen.

MAN-IN-THE-MIDDLE-ANGRIFF

Eine Art von Angriff, bei der ein Dritter die Kommunikation zwischen zwei Systemen aktiv abhört und kontrolliert.

> **Die Fabrik in Segnen hatte schon oft Probleme mit Malware und Viren in den Netzwerken der Steuerungssysteme, da Mitarbeiter ihre eigenen Laptops für Änderungen verwendeten oder Auftragnehmer neue Software auf Wechselmedien mitbrachten. Martin hielt das für einen weiteren Fall von Commodity-Malware und wies die Fabrik an, den normalen Betrieb fortzusetzen.**

Der CIO von Pulp Global ignoriert die Anzeichen eines Cyberangriffs; eBook „Der dunklen Seite einen Schritt voraus“

VERTEIDIGUNGSTAKTIK 5: TRANSPARENZ FÜR IHR NETZWERK UND IHR UNTERNEHMEN

ERKENNUNGS- UND REAKTIONSLÖSUNGEN (xDR)

Sind Sie in der Lage, festzustellen, welcher Benutzer in Ihrem Netzwerk eine bestimmte IP-Adresse zu einer bestimmten Tageszeit besucht hat? Können Sie ermitteln, wer in Ihrem Unternehmen eine bestimmte E-Mail erhalten hat? Langer Rede kurzer Sinn: Wenn Sie nicht wissen, was in Ihrem Netzwerk passiert, haben Sie zwangsläufig das Nachsehen. Sobald Sie aber einen Überblick haben, können Sie auf alles Verdächtige in Ihrer Infrastruktur reagieren.

Die besten Erkennungs- und Reaktionslösungen bieten kontextuelle Transparenz für ihre IT-Umgebung und den Sicherheitsstatus. Ohne Kontext sind einzelne Ereignisse bedeutungslos. Das Herstellen einer Verbindung zwischen einzelnen Ereignissen ist die einzige Möglichkeit, um schädliche Aktivitäten in Ihrer Infrastruktur zu erkennen. Durch das Wissen um die Vorgänge in Ihrem Netzwerk können Sie gezielte Cyberangriffe identifizieren und eindämmen.

SCHWACHSTELLENMANAGEMENT

Tools für das Schwachstellenmanagement geben Ihnen die geeigneten Mittel an die Hand, mit denen Sie Ihre Angriffsfläche mit dem Firmenwachstum im Blick behalten und auf Schwachstellen reagieren können, sobald sie auftreten. Mit der richtigen Lösung erhalten Sie einen Überblick über interne und externe Bedrohungen sowie die Schatten-IT.

Ein Großteil der Commodity-Malware nutzt Sicherheitslücken von Rechnern und Servern aus. Regelmäßiges Patchen dieser Ressourcen reduziert die Angriffsfläche und blockiert den einfachen Einstiegsweg für Hacker. Konzentrieren Sie sich zuerst auf das Patchen der geschäftskritischen Ressourcen.

Wir finden, dass Cybersicherheit mit umfassender Transparenz beginnt. Angreifer sollten Ihr Netzwerk nicht besser kennen als Sie selbst.

„Das interne Netzwerk von Pulp Global war ein Mischmasch verschiedener Systeme und Hosts aus drei Jahrzehnten. Darin war einfach alles enthalten – von Legacy-Anwendungen und -Servern bis hin zu brandneuen Windows-Systemen.

Viele der Systeme hatten bereits das Ende ihrer Lebensdauer überschritten und erhielten keine Software-Updates, was es für die Angreifer einfach machte, Zugang zu erhalten und sie mit öffentlich zugänglichen Exploits zu infizieren.

Keine Vorfallerkennung und ein schlechtes Schwachstellen-Management gefährden die Produktionssysteme von Pulp Global; eBook „Der dunklen Seite einen Schritt voraus““

VERTEIDIGUNGSTAKTIK 6: CYBERANGRIFFE IM KONTEXT INTERPRETIEREN

Hacker können sich tief in Ihrem Netzwerk vergraben, indem sie normale Betriebsabläufe so gut wie möglich nachahmen. Aber irgendwann müssen sie etwas tun – etwas Ungewöhnliches. Die einzige Frage ist, ob Sie aus den Hinweisen, die der Gegner hinterlässt, auch schlau werden.

Mit einer Erkennungs- und Reaktionslösung Ausschau nach ungewöhnlichen Vorgängen zu halten, ist der beste Weg, um gegen Datenlecks anzugehen. Auch verdächtige Einzelereignisse können bedeutsam sein, aber gerade bei hochentwickelten Angriffen sollte der Fokus hauptsächlich auf Aktivitäten liegen, die in einem verdächtigen Zusammenhang stehen.

Führt ein Endpunkt, der eine bestimmte Aktion zuvor noch nie ausgeführt hat, diese Aktion jetzt fortlaufend aus? Möglicherweise kann die gleiche Aktion an vielen Endpunkten im gesamten Unternehmen oder sogar in der externen Bedrohungslandschaft nachgewiesen werden. Finden ungewöhnliche Aktivitäten außerhalb der Bürozeiten statt?

Eine wirksame Erkennungs- und Reaktionslösung kann verdächtige Ereignisse und Warnungen in Zusammenhang setzen – auf Basis von interner IT-Umgebung, Cloud-Services und Bedrohungslandschaft. Alles, was Sie tun müssen, ist dann, genauer nachzuforschen oder die Reaktionsanleitung führender Erkennungs- und Reaktionslösungen zu befolgen.

> **„Die Fabrik in Segnen hatte schon oft Probleme mit Malware und Viren in den Netzwerken der Steuerungssysteme, da Mitarbeiter ihre eigenen Laptops verwendeten oder Auftragnehmer neue Software auf Wechselmedien mitbrachten. Martin hielt das für einen weiteren Fall von Commodity-Malware und wies die Fabrik an, den normalen Betrieb fortzusetzen.**

Verdächtige Ereignisse erregen die Aufmerk-samkeit eines Steuerungssystemingenieurs; eBook „Der dunklen Seite einen Schritt voraus“

VERTEIDIGUNGSTAKTIK 7: IMMER ZUERST DAS UNTERNEHMENSNETZWERK ABSICHERN

Der Schutz der wichtigsten Vermögenswerte Ihres Unternehmens – Ihrer Produktionsstätte, Ihres geistigen Eigentums, Ihrer vertraulichen Daten etc. – sollte immer mit der Absicherung des internen Netzwerks beginnen. Das interne Netzwerk ist stets die Stelle, an der Angreifer am häufigsten einsteigen.

Mit einer intelligenten, proaktiven Strategie zur Erkennung von Bedrohungen können Sie Angreifer enttarnen, bevor sie in Ihre kritischsten Systeme, etwa bis zu Ihren industriellen Steuerungen, vordringen. Eine wachsame Bedrohungserkennung nutzt die Kraft der KI, um die sprichwörtliche Nadel im Heuhaufen zu finden. Darüberhinaus nutzt sie auch die menschliche Intelligenz, um die gewonnenen Erkenntnisse zu verifizieren. Entscheiden Sie sich für eine hochpräzise Lösung. Je früher Sie einen Eindringling bemerken, desto geringer sind die Verluste für Ihr Unternehmen.

„Um dem Werkspersonal die Anmeldung bei den Hosts zu erleichtern, hatten die lokalen IT-Administratoren die Account-Passwörter in den Feldern vorausgefüllt. So konnten sie die Passwörter mit Benutzern teilen, die sie vergessen hatten. Neben den Standardbenutzern zählten auch einige Mitarbeiter mit Domain-Administrator-Konten zu diesem Personenkreis. Wie schon beim Unternehmensnetzwerk standen auch in diesem Fall der Gruppe von Number One die Türen wieder weit offen.“

Durch den Zugriff auf das Unternehmensnetzwerk kann der Angreifer in das Produktionsnetzwerk von Pulp Global gelangen; eBook „Der dunklen Seite einen Schritt voraus“

VERTEIDIGUNGSTAKTIK 8: AUF SICHERHEITSVORFÄLLE VORBEREITEN

Auch wenn Unternehmen das Risiko von Cyberangriffen verringern können und sollten, kann kein Unternehmen davon ausgehen, dass es völlig immun ist. Die Widerstandsfähigkeit gegen Angriffe beginnt damit, dass Sie die Tatsache akzeptieren, dass Ihr Unternehmen eines Tages Opfer eines Angriffs werden kann.

Ein resilientes Unternehmen bereitet sich auf einen Angriff vor, weiß, was zu tun ist, wenn es angegriffen wird, und geht gegen auch gezielt die Auswirkungen des Angriffs vor. Diese Fähigkeiten sollten geplant und geübt werden, und zwar lange bevor es tatsächlich zu einem Vorfall kommt.

DIE SCHLÜSSEL ZU CYBERRESILIENZ UND ERFOLGREICHEM VORFALLMANAGEMENT

Einsatzfähigkeit

Bereiten Sie sich darauf vor, mit allen Aspekten eines Vorfalls effizient umzugehen. Zuständigkeiten und Maßnahmen sollten klar definiert sein. Eine sorgfältige Vorbereitung mithilfe von Krisensimulationen hilft Ihnen, Lücken zu identifizieren und Abhilfemaßnahmen zu ergreifen, bevor es zu einem Vorfall kommt. Üben Sie die Vorgehensweisen regelmäßig und verbessern Sie die Effektivität Ihres Krisenmanagementteams im Umgang mit künftigen Vorfällen.

Reaktion

Eine schnelle Reaktion erfordert forensische Fähigkeiten. Außerdem benötigen Sie ein verlässliches Personal- und Prozessmanagement sowie eine effektive Kommunikation. Die Koordination und Untersuchung von Cybervorfällen erfordert regelmäßige Übungen und aktuellste Kenntnisse der Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures"; TTP) der Angreifer. Eine Unterstützung Ihres Teams durch erfahrene Berater minimiert die Auswirkungen von Datenlecks.

Wiederherstellung

Planen und üben Sie die erforderlichen Schritte, um zum normalen Betrieb zurückzukehren und den Schaden zu begrenzen. Die gewonnenen Erkenntnisse sollten in die Reaktionspläne für zukünftige Vorfälle einfließen.

" Während die Reaktion auf den Vorfall und die forensischen Untersuchungen fortdauerten, arbeiteten CEO und Vorstand am Kommunikationsplan für die Mitarbeiter, den Kundenstamm und die Medien. Nachdem der CEO die Erklärung veröffentlicht hatte, brach der Aktienkurs innerhalb eines einzigen Tages um mehr als zehn Prozent ein.

Pulp Global musste mitten im Chaos des Angriffs einen Plan für die Reaktion auf Vorfälle aufstellen; eBook „Der dunklen Seite einen Schritt voraus"

DIE BESTE KOMBINATION

Den Angreifern einen Schritt voraus zu bleiben, erfordert ein Aktivwerden an vielen Fronten. Wenn Sie Ihre Cybersicherheit nicht permanent überprüfen und verbessern, machen Sie sich zu einem leichten Ziel.

Präventive Technologien sind das Rückgrat Ihrer Sicherheit. Erkennungs- und Reaktionslösungen schaffen Transparenz. Ein waches Sicherheitsbewusstsein schützt vor den Manipulationstaktiken. Und falls es bei Ihnen zu Datenlecks kommen sollte, stellt schließlich ein geeigneter Vorfallreaktionsplan sicher, dass Sie sich schnell wieder davon erholen.

Es ist nicht einfach, mit der Cybersicherheit Schritt zu halten. Die gute Nachricht ist, dass Sie dabei nicht alleine dastehen. Arbeiten Sie mit erfahrenen externen Experten zusammen, und konzentrieren Sie Ihre Maßnahmen auf das, was für Ihr Unternehmen wichtig ist. Überprüfen Sie Ihre Cybersicherheitsmaßnahmen mit einem ganzheitlichen Ansatz – nicht nur in Bezug auf Produkte und Technologien, sondern auch auf Mitarbeiter und Prozesse. Wir Risiken kontrollieren will, muss Sicherheit als eine kontinuierliche Aufgabe betrachten.

Fakt ist, dass Sie nie zu 100 Prozent sicher sind. Bei der Entscheidung über Security-Investitionen ist die Schlüsselfrage, wie viel Risiko Ihr Unternehmen zu akzeptieren bereit ist. Das Risikomanagement ist Ihr Werkzeug, um Sicherheitsausgaben zu priorisieren und fundierte Entscheidungen zu treffen. Die richtigen Entscheidungen stärken Ihr Unternehmen und sichern seinen Fortbestand.

Je mehr sich Ihr Technologiestack entwickelt und je innovativer die Angreifer vorgehen, desto wichtiger ist es, dass Menschen die Cybersicherheitsstrategie vorgeben. Software allein wird mit dem Verhalten von Angreifern und mit menschlichem Versagen nicht fertig. Es braucht sowohl Software-Intelligenz als auch menschliche Expertise.

Die beste Lösung kombiniert beides: Mensch und Maschine.

Lesen Sie die ganze Geschichte über den Cyberangriff auf Pulp Global: eBook „Der dunklen Seite einen Schritt voraus“

F-SECURE – BLEIBEN SIE DEN KRIMINELLEN IMMER EINEN SCHRITT VORAUS

Niemand weiß mehr über Cybersicherheit als F-Secure. F-Secure ist seit drei Jahrzehnten ein Innovationstreiber im Bereich Cybersicherheit und schützt Zehntausende Unternehmen und Millionen Anwender. Mit unübertroffener Erfahrung in den Bereichen Endpoint Protection sowie Erkennung und Reaktion schützt F-Secure Unternehmen und Verbraucher gegen Bedrohungen jeder Art – von hochentwickelten Cyberangriffen und Datenschutzverletzungen bis hin zu umfangreichen Ransomware-Infektionen. Die ausgefeilte Technologie von F-Secure vereint die Stärken des maschinellen Lernens und die menschliche Expertise seiner weltweit anerkannten Sicherheitslabors zu einem einzigartigen Ansatz: Live Security.

Die Sicherheitsexperten von F-Secure waren an mehr Ermittlungen im Bereich der Cyberkriminalität in Europa beteiligt als jedes andere Unternehmen am Markt, und die Produkte von F-Secure werden von mehr als 200 Breitband- und Mobilfunkanbietern sowie von tausenden Vertriebspartnern weltweit verkauft.

F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

F-Secure