01

SCHUTZ VOR DEM ANGRIFF

SOFTWARE UND SYSTEME AUF DEM NEUESTEN STAND HALTEN

„Die Updates müssen kontinuierlich durchgeführt werden und Windows-PCs, aber auch Linux- und Mac-Systeme, die ebenfalls Einfallstore sein können, einschließen. Die gesamte Bürolandschaft ist betroffen, von Microsoft Exchange über das Active Directory bis hin zu allen exponierten Servern, auch wenn es sich um kleine handelt."

DATEN SICHERN ... UND BACKUPS SCHÜTZEN

„Diese Vorsichtsmaßnahme allein reicht nicht aus, da die Ransomware zuerst die Backups zu zerstören versucht, noch vor der Verschlüsselung. Die Sicherungsdateien dürfen nicht mit dem Computer verbunden sein und Backups müssen häufig durchgeführt werden. Außerdem muss die Wiederherstellung getestet werden, um sicherzustellen, dass die Sicherungsdateien brauchbar sind."

INFORMATIONSSYSTEME PARTITIONIEREN

„Dazu empfiehlt es sich, strenge Regeln für den zulässigen Datenfluss zwischen verschiedenen Bereichen je nach ihrer Kritikalität einzurichten."

BENUTZERRECHTE UND NUTZERBERECHTIGUNGEN EINSCHRÄNKEN

„In diesem Punkt ist das Zeitmanagement entscheidend: Um die Sicherheit aufrechtzuerhalten, muss man regelmäßige Überprüfungen einplanen."

PROTOKOLLÜBERWACHUNG IMPLEMENTIEREN

„Die Log-Sammlung ist ein Muss. In Fällen, in denen ein sehr hohes Sicherheitsniveau erforderlich ist, kann über ein SOC eine Komponente zur Erkennung von Eindringlingen hinzugefügt werden."

MITARBEITER SENSIBILISIEREN

„Mit dem Social Engineering ist das Haupteinfallstor in das Informationssystem eines Unternehmens immer noch die Belegschaft. Daher ist es wichtig, über Themen der Cybersicherheit zu sprechen, auch wenn die Sensibilisierung ihre Grenzen hat."

STRATEGIE FÜR DIE KRISENKOMMUNIKATION IM CYBERSPACE ENTWERFEN

„Auch hier ist es hilfreich, wenn man im Vorfeld an seinen Botschaften und Kontakten gearbeitet hat, um mit den verschiedenen Zielgruppen angemessen zu kommunizieren. Mitteilungen, die dazu dienen, z. B. vor einem ungeplanten Produktionsstopp zu warnen oder auch vor dem Verlust persönlicher Daten, wie in der DSGVO vorgesehen."

PLAN ZUR REAKTION AUF CYBERANGRIFFE UMSETZEN

„Dieser Plan ist entscheidend, da er eine schnelle Reaktion ermöglicht, indem zum Beispiel die zuvor identifizierten CERT-Firmen so früh wie möglich kontaktiert werden. Er umfasst natürlich auch eine technische Komponente mit der Einführung von Schutzlösungen wie Stormshield Endpoint Security Evolution und Stormshield Network Security."

NUTZEN EINER CYBER-VERSICHERUNG BEURTEILEN

„Einige Cyber-Versicherungen enthalten Klauseln, die den Einsatz von Cyber-Sicherheitslösungen vorschreiben, und sind in dieser Hinsicht interessant, da sie einen gewissen Schutz vorsehen. Dennoch sollte man die Cyberversicherung nicht als Überlebensmaßnahme sehen, die allein ausreicht, und schon gar nicht als Schutzmaßnahme. Mit anderen Worten: Eine Versicherung gegen Ransomware ist niemals eine Cybersicherheitsstrategie."

Ransomware: welche Strategien sollte man anwenden, um diese Geldmaschinen zum Entgleisen zu bringen?

Ransomware ist zum Sorgenkind der IT-Abteilungen und der Unternehmen im Allgemeinen geworden. Ist sie deshalb ein unabwendbares Schicksal? Wir fragen Sébastien Viou, Direktor für Produkt-Cybersicherheit und Cyberexperte von Stormshield, welche Maßnahmen ergriffen werden können, um dem entgegenzuwirken.

STORMSHIELD

02
SCHADENSBEGRENZUNG WÄHREND EINES ANGRIFFS

GUTE REFLEXE ANNEHMEN

„Man muss in der Lage sein, schnell zu erkennen, dass etwas nicht stimmt, und nicht davor zurückschrecken, den Stecker zu ziehen, um das Risiko zu mindern und die Ausbreitung so weit wie möglich einzudämmen. Auch auf individueller Ebene muss man lernen zu reagieren, zu sagen „Ich habe an der falschen Stelle geklickt", denn jede Minute zählt."

STEUERUNG DES CYBERKRISENMANAGEMENTS VOM VORSTAND

AUF DER RICHTIGEN EBENE KOMMUNIZIEREN

ANZEIGE ERSTATTEN

03
WIEDERHERSTELLUNG NACH EINEM ANGRIFF

SYSTEME AUS GESUNDEN QUELLEN WIEDERHERSTELLEN

NACHFORSCHUNGEN ÜBER DEN ANGRIFFSPFAD ANSTELLEN

„Um den Ablauf des Angriffs und die Schwachstellen des eigenen Systems zu verstehen, muss man analysieren, was passiert ist. Auf diese Weise schafft man sich die besten Voraussetzungen, um zu verhindern, dass so etwas noch einmal passiert."

KORREKTURPLAN ERSTELLEN

„Je nach Fall muss man vielleicht eine Multi-Faktor- Authentifizierung einführen oder die auf den Rechnern vorhandenen Sicherheitslösungen verbessern."

EINEN PRODUKTIONSPLAN ERSTELLEN, UM DEN RÜCKSTAND AUFZUHOLEN

STRAFVERFOLGUNG EINLEITEN, FALLS DIES NICHT BEREITS GESCHEHEN IST

UMGANG MIT DEN PSYCHOLOGISCHEN AUSWIRKUNGEN AUF DIE MITARBEITER

„Kurzarbeit, Schuldgefühle, Überlastung der IT-Teams – Ransomware hat auch Auswirkungen auf die menschlichen Ressourcen, die berücksichtigt werden müssen."

SETZEN SIE DEN KOMMUNIKATIONSPLAN BEI DEN BETROFFENEN KUNDEN, IHREN INVESTOREN USW. EIN.

FALL DER VERSICHERUNG VORLEGEN